ユーザ ガイド

SBG900J
ワイヤレス ケーブルモデム
ゲートウェイ

MOTOROLA
intelligence everywhere™

アラート：火災や感電を防ぐため、機器を雨や湿気の多い場所に設置しないでください。機器を水が滴ったり、跳ねたりする場所へ置かないでください。花瓶など、液体が入っている物を機器の上に置かないでください。

注意：本装置付属の電源アダプタを使用し、本装置を設置タイプの交流壁コンセントへ接続してください。

注意：本製品はシステムコンポーネント間の指定ケーブルを使用した状況下でテストを受け、承認されています。規制および安全性に準拠するため、付属しているインターフェースおよび電源ケーブルのみ使用し、それらを適切に設置してください。

注意：主供給回路への接続に異なる種類のコードを使用してもかまいません。使用国における全適用製品の安全性条件に準拠した主線コードのみ使用してください。

注意：本製品の設置は配線規格および地域の規制に準拠していなければなりません。

注意：ユニットを開かないでください。インストールおよびトラブルシューティング指示書にないサービスは行わないでください。サービスについては資格を有する保守要員に相談してください。

注意：弊社の許可無く本装置へ任意に変更および修正を加えた場合、使用者の本装置に対する使用権が失われることがあります。

本装置を使用する際、火災、感電および人身負傷の危険を軽減するため、以下を含む基本的な安全予防策が取られているべきです。

- 本装置の操作を行う前に、本項または取扱説明書をお読みください。すべての安全予防策に対し、特に気を付けてください。今後のため、指示書は保持してください。
- 本装置は本製品に付属する文書に記載されている製造元の指示に厳密に従い、インストールおよび使用されなければなりません。
- 指示書内のすべてのアラートおよび注意文に従ってください。本装置に添付されているすべてのアラートおよび注意記号を注視してください。
- 本装置に付属しているすべての指示文に従ってください。
- 火災または感電の危険があるため、コンセントまたは延長コードに多くのプラグを差し込み過ぎないでください。交流コンセント、延長コードの差し込み過ぎ、擦り切れた電源コード、損傷またはひびの入ったワイヤ被覆および損壊したプラグは危険です。感電および火災を発生させる危険性があります。
- コードを踏んだり、コードの上またはコードに対して置かれた物によって挟まれたりすることのないよう、電源コードを迂回させてください。電源コードがプラグまたは簡易コンセントに差し込まれている場合は特に注意してください。製品から出て行く場所を点検してください。
- 電源コードの長さと適合するよう、本装置を電気コンセントと十分近い場所に設置してください。
- 機器の電源コードまたはアダプタを交流壁コンセントから取り外せるよう、本装置を簡単に手の届く場所に設置してください。
- プラグの先端部分が見えることなく完全に差し込まれていない限り、プラグを延長コード、コンセント、または他のアウトレットへ差し込まないでください。
- 本装置は安定した場所に設置してください。
- 雷雨または稲妻が発生する危険がある時は、ケーブルモデムをインストールしないでください。
- *落雷中は、本製品を使用しないでください。*落雷による感電の危険があります。落雷中の更なる保護のため、または長期間使用せずに放置する場合、コードを壁コンセントから抜き取り、ケーブルシステムから取り外してください。これにより、落雷および電気サージによる本製品の損傷を防ぐことができます。

- 本装置をつなぐ交流コンセントへ、交流サージ保護器を設置することをお奨めします。落雷や他の電気的サージによる装置への損傷を防ぎます。
- 本装置を覆ったり他の物で空気の流れを塞いだりしないでください。本装置は、高温多湿をさけた場所や、振動およびほこりのない場所に設置してください。
- 装置は清潔で乾燥した布で拭いてください。クリーニング液あるいは類似した化学薬品は絶対に使用しないでください。機器へクリーナーを直接スプレーしないでください。ほこりを取り除くためには、エアスプレー等を使用してください。
- アースされた同軸ケーブルテレビ差込口へケーブルモデムを接続する時、同軸ケーブルに触れてモデムが静電気によって損傷することを避けてください。
- イーサネットケーブルをケーブルモデムまたは PC から切断または再接続する際、必ず最初にケーブルモデムにある同軸ケーブルコネクタに触れてください。
- 本製品の操作には、本製品に表示されている電源種類のみ使用してください。ご自宅に供給されている電源の種類がわからない場合、販売元あるいは地域の電気会社にご相談ください。

FCC 適合 クラス B デジタル装置

本装置は FCC 規定第 15 項の条件を満たしています。操作は以下の二つの条件の対象となります。(1) 本装置は有害な混信を引き起こさず、(2) 本装置は希望しない動作を引き起こす可能性のある混信を含む、いかなる混信の受信をも許容しなければなりません。

注 : 当装置は FCC 規定第 15 項のクラス B デジタル装置としてのテストを受け、その条件を満たしています。これらの条件は、当装置を住宅地域において操作する上で、有害な混信から保護されるよう定められています。本装置は高周波数を発生、使用、放射しますので、指示書通り正しくインストールされていない場合は有害なラジオ混信を招く恐れがあります。ただし、正しくインストールが行われている場合においても、絶対に有害混信を招かないという保証はありません。本装置がラジオもしくはテレビ受信に対して混信を招き、装置の電源の入切を行うことで、本装置が原因であることが明らかである場合は、以下の 1 つまたはそれ以上の措置に従い、混信の修正を試みてください。

- 受信アンテナの方向修正、または再配置を行う。
- 本装置と受信機の間隔を広げる。
- 本装置を、受信機が接続されているものとは別の電源に接続し直す。

FCC 認可

本製品には無線伝送装置が含まれ、それに従いラジエータに関する国際 FCC 規則の 47 CFR 第 15 条に準拠するよう認可されています。無線伝送装置を含まない製品は FCC ID および FCC ロゴに表示されています。

注意：高周波への照射。

FCC の RF（高周波）への照射準拠必要条件に準拠するためには、アンテナおよび人体の一部（手、手首、足、足首を含む）との距離間隔が少なくとも 20 cm（8 インチ）離れていなければなければなりません。

カナダ - カナダ産業省 (IC)

本機器のワイヤレス無線はカナダ産業省の RSS210 および RSS102 に準拠しています。

このクラス B デジタル機器はカナダ ICES-003 に準拠しています。

無線妨害を防ぐため、本機器は最大限の保護のため室内の窓から離れた場所で使用することを意図しています。室外に設置されている装置（または送信アンテナ）には許可が必要です。

本製品と共に提供されているアンテナまたはモトローラ社によって認可されているアンテナのみご使用ください。

規制、安全性、ソフトウェア ライセンスおよび保証情報

- *規制、安全性、ソフトウェア ライセンスおよび保証*に関する情報カードに記載されている事項を除き、本製品についてモトローラ社によるいかなる保証もないものとします。モトローラ社の保証はご加入のサービスプロバイダーによって改造または再発行された製品には適用されません。
- この装置は、情報処理装置等電波障害自主規制協議会 (VCCI) の基準に基づくクラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

© 2004 モトローラ株式会社

All rights reserved. モトローラ社の文書による許可無く、この出版をいかなる形式または方法によって複製、またはそれに基づく二次的著作物（翻訳、変更、改作等）の作成を行うことはできません。

モトローラ社には出版物を改訂する権利があり、モトローラ社は改訂および変更の通知の義務なく時として内容の変更を行えるものとします。モトローラ社はこのガイドを、明示または黙示に関わらず、商品性、特定目的への適合性を含む（但し、必ずしもこれらに限定されない）、いかなる保証を負担することなく提供します。モトローラ社は本取扱説明書に記載されている製品への改善および変更を随時行えるものとします。

モトローラおよび M 形状のロゴはアメリカ合衆国特許および登録商標庁に登録されています。マイクロソフト (Microsoft)、ウィンドウズ (Windows)、Windows Me、Windows NT および Xbox はマイクロソフト社の登録商標です。Windows XP および Xbox*Live* はマイクロソフト社の商標です。マイクロソフト ウィンドウズ画面はマイクロソフト社の許可を得て掲載しました。マッキントッシュ (Macintosh) および AppleTalk はアップル社 (Apple Computer) の登録商標です。Iomega は Iomega 社の登録商標です。Linux は Linus Torvalds の登録商標です。Acrobat Reader はアドビ システムズ (Adobe Systems) 社の登録商標です。ネットスケープ (Netscape) およびナビゲーター (Navigator) はネットスケープ コミュニケーションズ コーポレーション社 (Netscape Communications Corporation) の登録商標です。PlayStation は株式会社ソニー・コンピュータエンタテインメントの登録商標です。UNIX はアメリカ合衆国および他の国において、オープングループ (Open Group) の登録商標です。Wi-Fi は Wi-Fi Alliance の登録商標です。他の全製品またはサービス名は各所有者に属しています。

目次

目次 v

概要 1
簡単な設定 2
ネットワーク接続の種類 2
一つの機器でパワフルな機能 3
フロントパネル 4
リアパネル 5
SBG900J の底面ラベル 6
SBG900J LAN の選択 6
有線イーサネット LAN 7
セキュリティ 8
ファイヤーウォール 8
DMZ 9
ポート トリガリング 9
ワイヤレス セキュリティ 9
ポート フォワーディング 10
仮想プライベート ネットワーク 10

基本設定 11
SBG900J 設定プログラムの開始 12
デフォルト パスワードの変更 14
リモートアクセスの有効化 15
ヘルプの使用 16
ファイヤーウォール ポリシーの設定 17
ファイヤーウォール > ポリシー— 詳細ページ 19
ファイヤーウォール > アラート— 基本ページ 21
ファイヤーウォール > アラート— E メールページ . 22
ファイヤーウォール > ログページ 23

ゲートウェイの設定 24
ゲートウェイの有効化 25
ゲートウェイ > ステータスページ 26
ゲートウェイ > WAN ページ 27
ゲートウェイ > LAN — NAT 設定ページ 29
ゲートウェイ > LAN — DHCP サーバ設定ページ 30
ゲートウェイ > LAN — DHCP リースページ 31
ゲートウェイ > ポート フォワーディング— ステータスページ 32
ゲートウェイ > ポート フォワーディング— 設定ページ 33
ゲートウェイ > ポートトリガー 定義済みページ 34
ゲートウェイ > ポートトリガー カスタムページ 36
ゲートウェイ > ログページ 37

ワイヤレス LAN を設定する 38
SBG900J で WPA を設定する 40
SBG900J で WEP を設定する 42
ワイヤレス LAN アクセスの制限 44
SBG900J でワイヤレス ネットワーク名を設定する 45
SBG900J の MAC アクセス制御リストを設定する 47
ワイヤレス クライアントを設定する 48
WPA 用にワイヤレス クライアントを設定する . . . 49
WEP 用にワイヤレス クライアントを設定する . . . 49
ワイヤレス クライアントにネットワーク名 (ESSID) を設定する 49
SBG900J 設定プログラムのワイヤレスページ 50
ワイヤレス > ステータスページ 51
ワイヤレス > ネットワークページ 52
ワイヤレス > セキュリティ— 詳細ページ 53
ワイヤレス > セキュリティ— 詳細ページ 55
ワイヤレス > 統計ページ 56

トラブルシューティング 58
フロントパネルライトおよびエラー状態 59

お問合せ先 60

よくある質問 (FAQ) 61

仕様 62

用語集 64

ソフトウェア ライセンス 83

概要

ご家庭、ホームオフィス Motorola® SURFboard® ワイヤレス ケーブルモデムゲートウェイ SBG900J をご利用いただき、ありがとうございます。以下の場所において、SURFboard ゲートウェイ (SBG900J）は特に便利です：

- 複数のコンピュータをインターネットおよび相互接続する必要があるご家庭
- 高速、経済的、および安全性の高いインターネットアクセスを必要とする小企業またはホームオフィス

お使いの SBG900J と機能および外見は写真と異なる場合があります。

- DOCSIS® ケーブルモデム、IEEE 802.11g ワイヤレスアクセス ポイント、イーサネット 10/100Base-T 接続およびアドバンスト ファイヤーウォールの 4 つの異なる製品を、1 つのコンパクトな製品へと合わせました
- ケーブルを使用または使用せずに、一つのブロードバンド接続、ファイルおよび周辺機器を共有するカスタム ネットワークを作ることができます
- 高度なファイヤーウォールにより、有線ユーザーまたはワイヤレス ユーザーへ拡張ネットワークセキュリティを提供します

本製品は予告なしに変更されることがあります。

簡単な設定

- 基本操作にはほとんどのデフォルト設定がそのまま使用できるため、設定を変更する必要がありません。ケーブルテレビ局によっては MAC アドレス登録が必要な場合がございます。
- 設定プログラムはグラフィカル ユーザー インターフェース (GUI) を使用しているため、ワイヤレス、イーサネット、ルータ、DHCP およびセキュリティ設定に必要な環境設定を簡単に行うことができます。セットアッププログラムの使用に関して詳しくは、「基本設定」を参照してください。

ネットワーク接続の種類

SBG900J は、お使いのコンピュータでデータを交換するための、色々なネットワーク接続の種類を提供しています。コンピュータおよび SBG900J 間を、ワイヤレスまたは有線接続、あるいは両方を組み合わせて接続することができます。ネットワークとして、以下のネットワーク接続の一つまたはそれらを組み合わせることができます。

- イーサネット ローカル エリア ネットワーク
- ワイヤレス LAN（IEEE 802.11b ワイヤレスクライアントもサポートする IEEE 802.11g）

一つの機器でパワフルな機能

SBG900J では、高速インターネットアクセス、ネットワーキングおよびコンピュータセキュリティを一体化させました。SBG900J には以下の特徴があります。

- ケーブルインターネットは常時接続のブロードバンドアクセスのため、従来のダイヤルアップまたは ISDN モデムに比べ高速なデータ転送を提供できます。
- 一つのブロードバンド接続で、最高 253 台のコンピュータがウェブをサーフすることができます。LAN 上のすべてのコンピュータが同じ物理的ネットワークに接続されているかのように通信します。
- ノートコンピュータ ユーザーは接続したままにご家庭または小規模オフィスを移動できます。また、ネットワーク配線を行うことなく、デスクトップ コンピュータを接続することができる、IEEE 802.11g ワイヤレス アクセス ポイント 距離により、ワイヤレス接続の速度はイーサネット接続と一致させることができます。
- 10/100Base-T イーサネットポートは半二重および全二重。接続および AUTO-MDIX をサポートしております。
- ワイヤレス LAN (WLAN) または有線イーサネット LAN 用のルーティング。ハブを使用した 1 台以上のコンピュータを接続することができます。
- 有線またはワイヤレス を組み合わせた DHCP サーバー機能は LAN を簡単に設定できます。
- ステートフル インスペクション、侵入検知、DMZ、Dos (denial-of-service) 攻撃の予防、およびネットワーク アドレス変換 (NAT) をサポートするアドバンストファイヤーウォール。
- インターネットを経由したリモートアクセスのための VPN、IPSec、PPTP や L2TP をサポートしています。
- 特別なネットワーク必要条件を持つアプリケーションを実行するためのポートを設定するポート フォワーディング

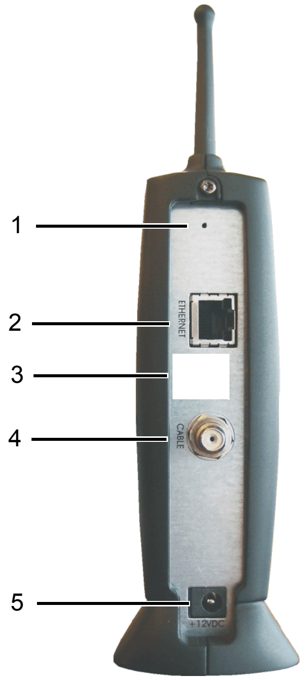
フロントパネル

フロントパネルにはインジケータ ライトがあります。*お使いの SBG900J は、図およびこのガイドにあるスクリーン画像と異なる場合があります。*

キー	ライト	点滅	オン
1	POWER	点滅しない	電源は正常に動作しています
2	RECEIVE	受信（ダウンストリーム）チャンネル接続をスキャン中	ダウンストリーム チャンネルへ接続されています
3	SEND	送信（アップストリーム）チャンネル接続をスキャン中	アップストリーム チャンネルへ接続されています
4	ONLINE	ネットワーク接続をスキャン中	スタートアップのプロセスが完了し、SBG900J はオンラインになっています
5	PC/ACTIVITY	インターネットでデータ転送または受信中	コンピュータまたは他の機器がイーサネット ポートに接続されています
6	WIRELESS	ワイヤレス アクティビティ	ワイヤレス インターフェースがオンになっています（SBG900J 設定プログラムのワイヤレス > ネットワークページ。でワイヤレスインターフェース有効化が選択されています）

リアパネル

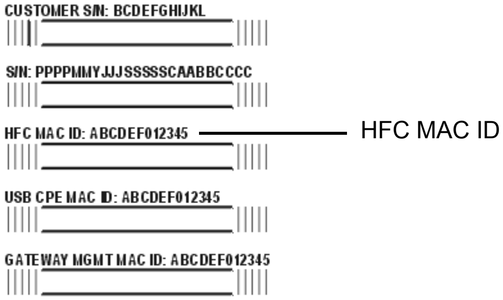
リアパネルにはケーブルコネクタ、リセットボタン、電源コンセントがあります。



キー	項目	説明
1	•	問題が発生した場合、このくぼんだボタンを押し、SBG900J を再起動することができます。(「トラブルシューティング」を参照してください)。すべての値をデフォルト値へリセットするには、ボタンを 5 秒以上押し続けてください。SBG900J は適切な通信チャンネルを取得した後ロックしなければならないため、リセットには 5 〜 30 分ほどかかります。
2		RJ-45 コネクタ付きイーサネット LAN ケーブルをイーサネット搭載コンピュータ、ハブ、ブリッジへ接続する際に、**ETHERNET** ポートを使用します。
3		このポートは使用できません。
4		同軸ケーブル（コアックス）差込口です。抜かないでください。
5		外部電源への **+12VDC** 電源コネクタを使用します。

SBG900J の底面ラベル

HFC MAC ID と印刷されている MAC アドレスをテクニカルサポート対応時などに、ご確認いただく場合がございます。



SBG900J LAN の選択

SBG900J は最大 253 台のクライアント コンピュータを以下の組み合わせによって接続することができます。

- 有線イーサネット LAN

各コンピュータには適切なネットワークアダプタハードウェアおよびドライバソフトウェアが必要です。イーサネット、ワイヤレスのクライアントは以下を共有することができます。

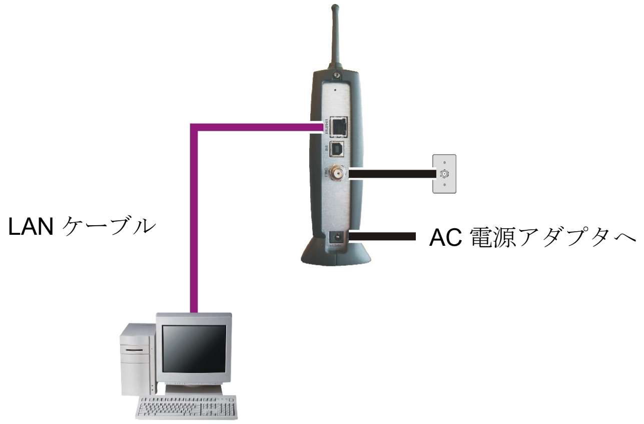
- ケーブルプロバイダーの使用条件に従った、一つのケーブル プロバイダー アカウントによるインターネットアクセス
- ファイル、記憶装置、マルチ- ユーザー ソフトウェア アプリケーション、ゲームおよびビデオ会議

ワイヤレスまたは有線ネットワーク接続は、ファイルおよび CD-ROM ドライブ、フロッピー ディスク ドライブおよび Iomega® ZIP ドライブなどの周辺機器の共有に Windows ネットワーキングを使用します。

有線イーサネット LAN

10/100Base-T イーサネット LAN 上の各コンピュータにはイーサネット ネットワーク インターフェース カード (NIC) およびドライバソフトウェアがインストールされている必要があります。SBG900J イーサネット ポートは auto-MDIX をサポートしているため、ストレートまたはクロスケーブルを使用して、ハブまたはコンピュータを接続することができます。すべてのイーサネット接続にはカテゴリ 5 のケーブルを使用します。

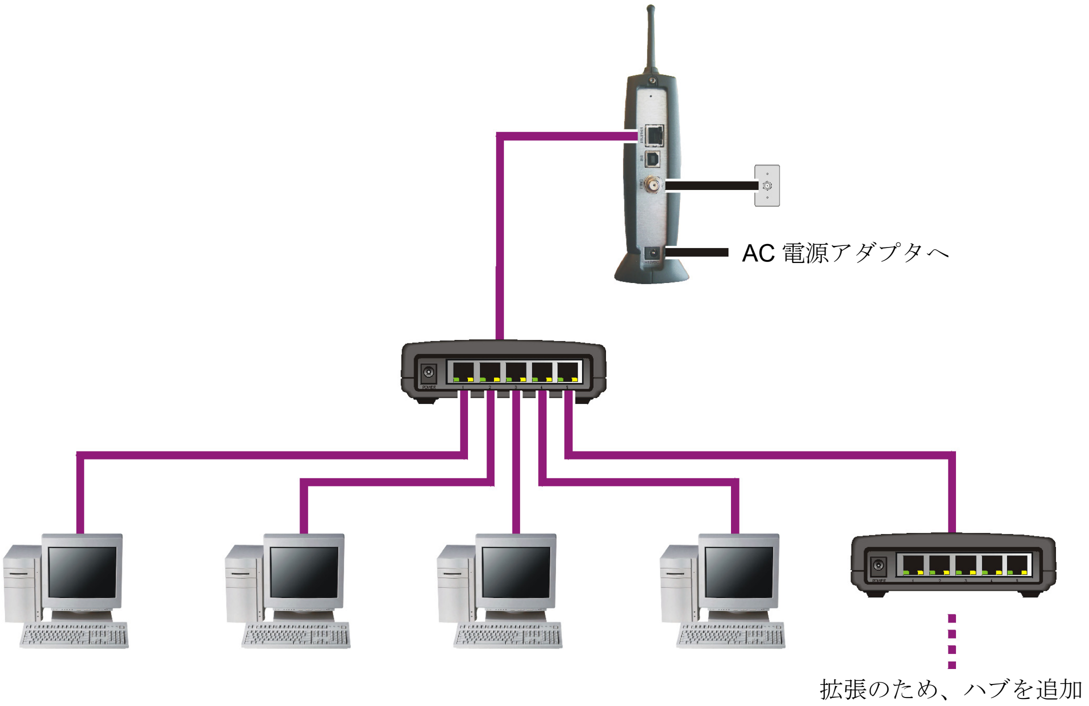
イーサネットからコンピュータへの接続例



1 台以上のコンピュータを接続した有線イーサネット LAN には 1 台またはそれ以上のハブが必要となります。ハブを SBG900J 上のイーサネットポートへ接続することができます。

以下の図は、SBG900J を使用して設定できるイーサネット LAN の例です。場所に適した方法で LAN をケーブルで接続します。イーサネットの配線については、イーサネット機器の取り扱い説明書をご参照ください。

ハブへのイーサネット接続の例



セキュリティ

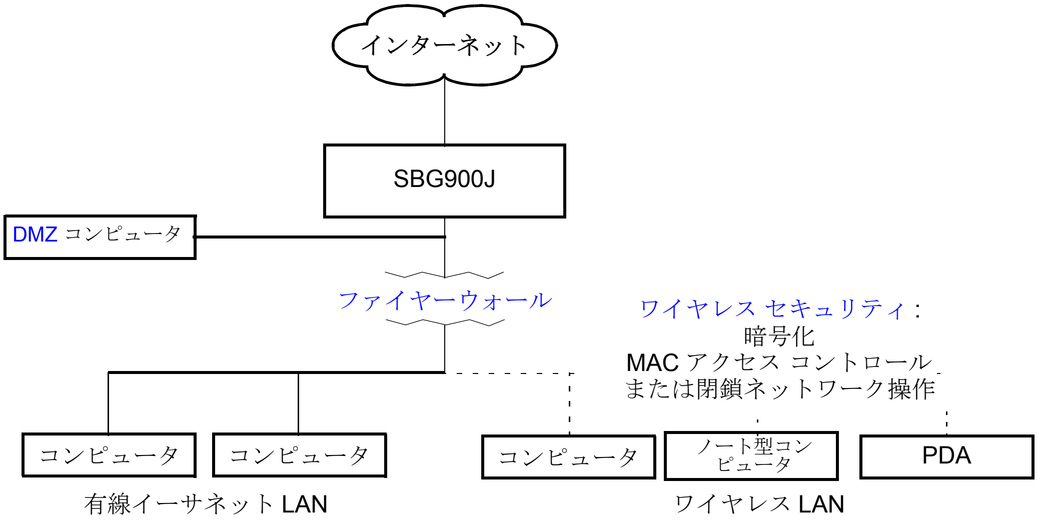
SBG900J は以下を提供します。

- SBG900J LAN をインターネット上の望まない攻撃から保護するためのファイヤーウォール
- ワイヤレス伝送用の、データ暗号およびネットワーク アクセス コントロール

ネットワーク アドレス変換 (NAT) は、SBG900J LAN コンピュータの IP アドレスをインターネット上で不可視にするため、セキュリティを提供します。

このダイアグラムは必ずしもネットワーク配線と一致しません。

物理的ネットワークのダイアグラムで表される SBG900J のセキュリティ対策



ファイヤーウォール

SBG900J ファイヤーウォールはインターネット上の望まない攻撃や、インターネットからの他の侵入から SBG900J LAN を保護します。侵入検知、セッショントラッキング、Dos (denial-of-service) 攻撃の予防をサポートするアドバンスト統合ステートフル インスペクションファイヤーウォールを提供します。ファイヤーウォールは、

- OSI ネットワークおよびトランスポート層上の各 TCP/IP セッションで、状態データを維持します。
- すべての送受信パケットを監視し、ファイヤーウォール ポリシーをそれぞれに適用することで不適切なパケットおよび侵入の試みを遮断します。
- 以下のすべてに対する、広範囲に渡るログを提供します。
  - — ユーザー認証
  - — 拒否された内部および外部接続要求
  - — セッション作成および終了
  - — 外部からの攻撃（侵入探知）

ポート使用の規則を設定するために、ファイヤーウォール フィルタを設定することができます。定義済みファイヤーウォール ポリシー テンプレートの選択について詳しくは、「ファイヤーウォール ポリシーの設定」を参照してください。

DMZ

非武装地帯 (DMZ) は、SBG900J LAN およびインターネット間で、論理的にファイヤーウォール外に位置する 1 台またはそれ以上のコンピュータです。DMZ は、外部ユーザーによるプライベートデータへの直接アクセスを防ぎます。

例えば、ネットワーク上の機密内容を開示することなく外部ユーザーがウェブサイトへアクセスできるよう、DMZ コンピュータ上のウェブ サーバーを設定することができます。

DMZ は、ファイヤーウォールを通して実行する場合に問題のある双方向ゲームをする際にも便利です。他のネットワークを保護しながら、ゲームで使用するコンピュータのみインターネットへ露出することができます。

ポート トリガリング

インターネットへアクセスするアプリケーションを実行する場合、通常インターネット上のコンピュータとの通信を初期化します。特にゲームなどのアプリケーションでは、インターネット上のコンピュータもお使いのコンピュータとの通信を初期化します。NAT は一般的にこれらの受信接続を許可しないため、

- SBG900J では、共通アプリケーション用のポート トリガリングが既に設定されています。
- 必要があれば、ゲートウェイ > ポートトリガー カスタムページで追加ポート トリガを設定することができます。

ワイヤレス セキュリティ

WLAN データは無線信号を使用して伝送されるため、何らかの対処を行わないと権限のない人物がお使いの WLAN へアクセスする可能性があります。*LAN 上における送信データの不正盗聴を防ぐため、ワイヤレス セキュリティを可能にしなければなりません。SBG900J のデフォルト設定では、不正侵入からのネットワークデータ保護または送信データのセキュリティが提供されていません。*

SBG900J は「ワイヤレス LAN を設定する」で記載されている通り、以下のワイヤレス セキュリティ対策を提供しています。

- ワイヤレス インターフェースにおける不正盗聴を防ぐため、以下の方法の *1* つを使用して伝送データを暗号化しなければなりません。
  - すべてのワイヤレス クライアントが Wi-Fi® 保護アクセス (WPA) 暗号化をサポートしている場合、WPA の使用を推奨いたします(「SBG900J で WPA を設定する」および「WPA 用にワイヤレス クライアントを設定する」を参照してください)
  - それ以外の場合は、SBG900J および各 WLAN クライアントで Wired Equivalency Privacy (WEP) キーを設定してください(「SBG900J で WEP を設定する」を参照してください)
- LAN データを不正侵入から保護するため、以下の 1 つまたは両方を持つコンピュータに WLAN アクセスを限定することができます。
  - わかっている MAC アドレス(「SBG900J の MAC アクセス制御リストを設定する」を参照してください)
  - SBG900J と同じ固有ネットワーク名 (ESSID)(「SBG900J でワイヤレス ネットワーク名を設定する」および「ワイヤレス クライアントにネットワーク名 (ESSID) を設定する」を参照してください)

同じネットワーク名を持つコンピュータのみにアクセスを制限することを、「ESSID ブロードキャスティングの無効化」と呼びます。

ポート フォワーディング

SBG900J は、LAN 上のコンピュータが E メールメッセージやウェブデータをインターネットへ送信する際に、論理データ ポートを開きます。論理データ ポートはイーサネット ポートなどの物理ポートとは異なります。プロトコルからのデータは一定のデータ ポートを通過しなければなりません。

ゲームおよびビデオ会議などのアプリケーションによっては、複数のデータポートを必要とするものがあります。NAT を有効にした場合、NAT はポートの一つから送信されたデータは同じポートへ戻されると想定するため問題を引き起こします。特別な必要条件を持つアプリケーションを実行するためには、ポート フォワーディングを設定する必要がある場合があります。

ポート フォワーディングを設定するには、インバウンドデータ用に開かれているインバウンド（ソース）ポートまたはポートの範囲を指定しなければなりません。ゲートウェイ > ポート フォワーディング― 設定ページを使用して、最大 32 ポート フォワーディングを設定することができます。

仮想プライベート ネットワーク

SBG900J はインターネット上で安全に遠隔コンピュータを接続するため、複数のトンネル VPN パススルー操作をサポートしています。SBG900J は、

- Point-to-Point トンネリング プロトコル (PPTP) およびレイヤ 2 トンネリング プロトコル (L2TP) と互換性があります。
- どの IPSec クライアントまたはゲートウェイおよび ANX 認可 IPSec スタックとも完全な相互操作が可能です。

基本設定

以下のセクションには SBG900J の基本設定についての情報が記載されています。

- SBG900J 設定プログラムの開始
- デフォルト パスワードの変更
- ヘルプの使用
- ファイヤーウォール ポリシーの設定

以下の注意文は、注意すべき問題点の要約です。

注意！

不正設定を防ぐため、SBG900J を最初に設定する際にデフォルトのパスワードを*直ちに*変更してください。「デフォルト パスワードの変更」を参照してください。

ファイヤーウォール機能をご利用頂く場合は、できるだけ安全性の高いファイヤーウォール ポリシーを選択してください。「ファイヤーウォール ポリシーの設定」を参照してください。

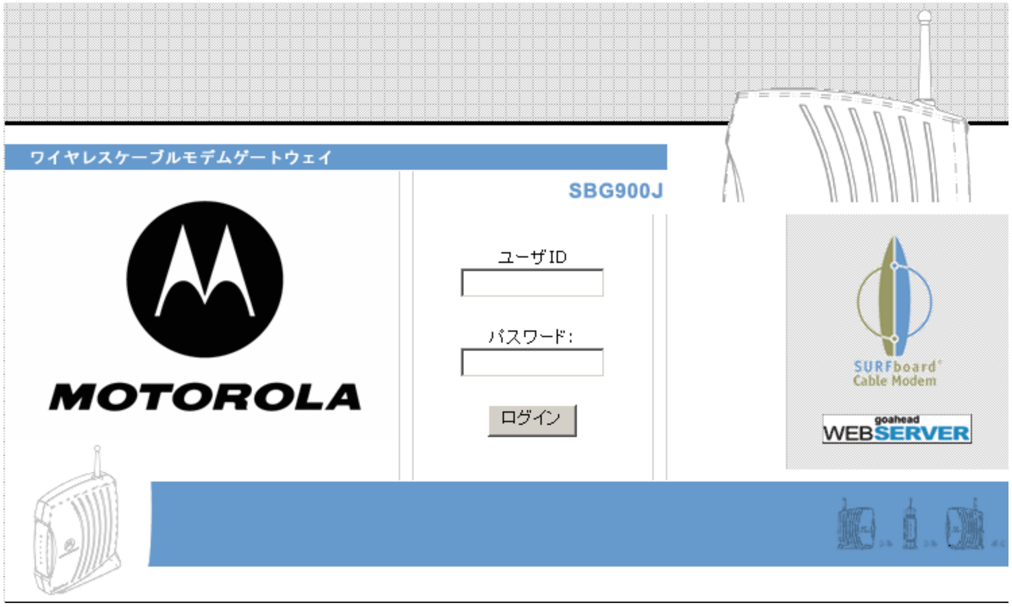
*有線 LAN のみを使用し、ワイヤレス クライアントがない場合、ワイヤレス > ネットワークページでワイヤレスインターフェース有効化*をオフにし、ワイヤレス インターフェースを無効にしてあることを確認します。

ワイヤレス LAN を使用する場合のみ、「ワイヤレス LAN を設定する」の指示に従ってください。

SBG900J 設定プログラムの開始

1 SBG900 へ配線されているコンピュータ上で、ウェブブラウザを開きます。*ワイヤレス接続では SBG900 の設定は行えませんのでご注意ください。*

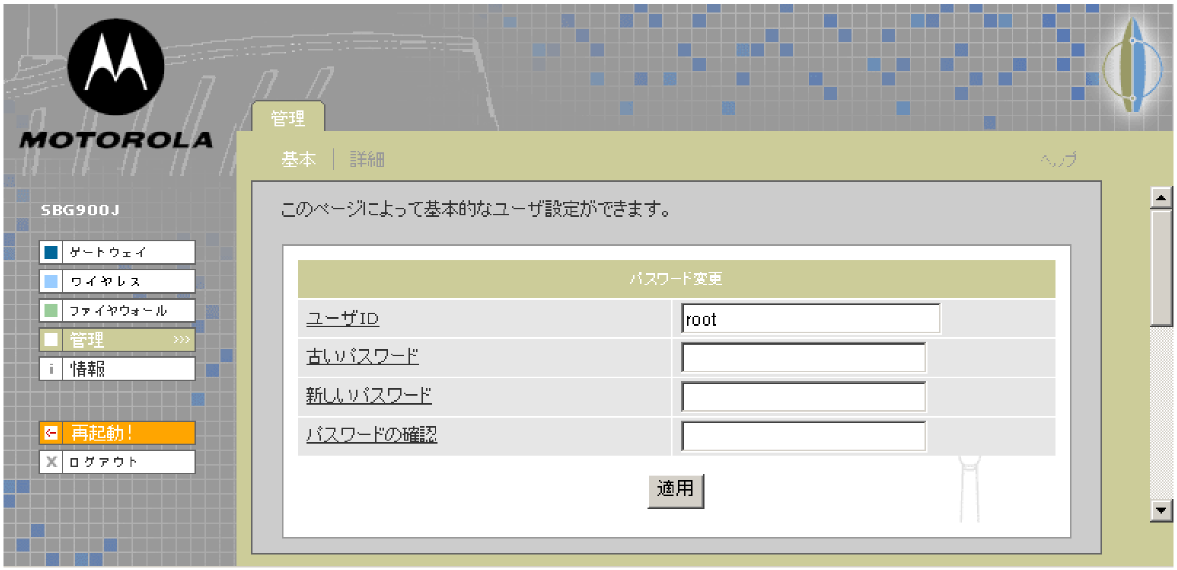
2 **ログイン**ウィンドウを表示するには、アドレスまたは場所フィールドへ **http://192.168.100.1** と入力し、**ログイン**を押します。



3 **ユーザー ID** フィールドへ*ユーザー名*を入力します。デフォルト値は「root」です（このフィールドでは大小文字を区別します）。

4 **パスワード**フィールドへ*パスワード*を入力します。デフォルト値は何も設定されていません。（ブランクでログインできます。）

5　**Log In**（ログイン）をクリックし、SBG900J 設定プログラムを表示します。



メニュー	説明
ゲートウェイ	ゲートウェイのオプションを設定および監視します（「ゲートウェイの設定」を参照）。
ワイヤレス	ワイヤレス インターフェースのオプションを設定および監視します（「ワイヤレス LAN を設定する」を参照）。
ファイヤーウォール	ファイヤーウォールを設定および監視します（「ファイヤーウォール ポリシーの設定」を参照）。
管理	デフォルト パスワードの変更
情報	SBG900J 設定プログラムについての情報を表示します。
再起動	SBG900J を再起動します。リアパネルにある RESET ボタンを 5 秒間以下押しても再起動します。
ログ アウト	SBG900J からログアウトします。

SBG900J 設定プログラムが開始できない場合、「トラブルシューティング」の情報を参照してください。

設定によっては、フィールドを変更し適用をクリックした後、変更を有効にするために再起動しなければならないことのアラートが表示されます。再起動には約 10 ～ 15 秒かかります。再起動後、もう一度ログインする必要があります。

デフォルト パスワードの変更

注意！

不正設定を防ぐため、SBG900J ワイヤレス ケーブルモデムゲートウェイを最初に設定する際にデフォルトのパスワードを*直ちに*変更してください。

デフォルト パスワードを変更するには、

1 **管理**をクリックし、管理— 基本ページを表示します。

2 **古いパスワード**フィールドに、古い*パスワード*を入力します。デフォルトパスワードは設定されておりません。

3 **新しいパスワード**フィールドに、新しい*パスワード*を入力します。

4 **パスワードの確認**フィールドに、新しい*パスワード*をもう一度入力します。

5 **適用**をクリックし、変更をします。

リモートアクセスの有効化

インターネットから SBG900J へリモートアクセスすることができます。インターネットから設定プログラムを実行するには、**ユーザー ID**、**パスワード**および SBG900J に割り当てられている**外部アドレス**が必要となります。リモートアクセスにより、リモートクライアント上のウェブ ブラウザを使用し、SBG900J のウェブサーバーへ接続することができます。

SBG900J へのリモートアクセスを有効にするには :

1 SBG900J 設定プログラムの左パネルで、**管理**をクリックし、管理— 基本ページを表示します。

2 **詳細**をクリックし、管理— 詳細ページを表示します。

3 **リモート アクセスの有効化**を選択します。

4 **適用**をクリックし、変更を適用します。

注意！

リモートアクセスを有効にすることにより、お使いのネットワーク上にないインターネット ユーザーがネットワーク設定を表示したり修正したりする際に、SBG900J へログオンすることができます。*必要がない限り、リモートアクセスを有効にしないことをお奨めします。リモートアクセスの必要がなくなったら直ちに設定を無効にするようお奨めします。*

ヘルプの使用

下線の付いた項目またはフィールドに関するヘルプを表示するには、そのテキストをクリックします。例えば、管理— 基本ページのフィールドまたはヘルプボタンをクリックすると、以下のようなヘルプが表示されます。

スクロールしてヘルプを参照するか、他の項目をクリックし、その項目のヘルプを表示することができます。

ファイヤーウォール ポリシーの設定

SBG900J ファイヤーウォールはインターネット上の望まない攻撃や、インターネットを経由した外部から SBG900J LAN を保護します。本セクションではファイヤーウォール > ポリシー ― 基本ページを使用して、SBG900J に付属している定義済みファイヤーウォール ポリシー テンプレートから一つを選択する方法について記載されています。

注意！

できるだけ安全度の高いファイヤーウォール ポリシーを選択してください。簡単ネットワーク設定を有効にするため、デフォルト ファイヤーウォール ポリシーはなしに設定されています。この設定ではセキュリティは提供されません。

SBG900J ファイヤーウォールで処理されるすべてのパケットに対する定義済みポリシーを選択するには、

1 SBG900J 設定プログラムの左パネルで、**ファイヤーウォール**をクリックします。
2 ポリシーをクリックします。
3 基本をクリックし、定義済みファイヤーウォール ポリシー テンプレートを表示します。

4 できるだけ安全性の高いファイヤーウォール ポリシーを選択してください。

高　最も安全な定義済みファイヤーウォール ポリシー テンプレートであり、最高のセキュリティを提供します。

中　定義済みファイヤーウォール ポリシー テンプレートは中程度の危険を含む一般的な設定を提供します。

低　定義済みファイヤーウォール ポリシー テンプレートは最小限のセキュリティを提供し、侵入の危険性が最も高くなります。

カスタム　ファイヤーウォール > ポリシー― 詳細ページで、*カスタム ファイヤーウォール ポリシーを作成する必要がある場合があります。カスタム ポリシーに関する必要知識があり、作成する必要がある場合を除き、カスタム ポリシーを作成しないでください。*

なし　ファイヤーウォールを無効化します。簡単ネットワーク設定を有効にするため、この設定がデフォルトになっています。*ネットワークを設定した後、セキュリティを改善するため高、中または低を設定してください。*

5 適用をクリックし、変更を適用します。

フィールドを変更し適用をクリックした後、変更を有効にするために再起動しなければならないことのアラートが表示されます。再起動には約 10 ～ 15 秒かかります。再起動後、もう一度ログインする必要があります。

- 高、中または低の定義済みポリシー テンプレートの規則を表示するか、ファイヤーウォール > ポリシー— 詳細ページでカスタム ポリシーを作成することができます。
- ファイヤーウォール > アラート— 基本ページおよびファイヤーウォール > アラート— E メールページでファイヤーウォールアラートを設定することができます。
- ファイヤーウォール > ログページでファイヤーウォールのログを表示することができます。

定義済みポリシーは SBG900J LAN 上のコンピュータへアウトバウンド インターネットアクセスを提供します。SBG900J ファイヤーウォールはステートフル インスペクションを使用して、データの流れに対応したアウトバウンド セッションがすでに実行されている場合、インバウンド応答を許可します。例えば、ウェブ ブラウザを使用する場合、アウトバウンド HTTP 接続はポート 80 で許可されます。アウトバウンド セッションが確立されているため、インターネットからのインバウンド応答が許可されます。

必要があれば、最初にアウトバウンド セッションを確立することなくインバウンド パケットを許可するよう、SBG900J ファイヤーウォールを設定することができます。ゲートウェイ > ポート フォワーディング— 設定ページでポート フォワーディング項目を設定するか、ゲートウェイ > LAN — NAT 設定ページで DMZ クライアントを設定する必要があります。

ファイヤーウォール > ポリシー— 詳細ページ

「ファイヤーウォール ポリシーの設定」で記載されている通り、定義済みポリシー テンプレートから一つ選択します。*カスタム ファイヤーウォール ポリシーに関する必要知識があり、作成する必要がある場合を除き、カスタム ポリシーを作成しないでください。*

カスタム ファイヤーウォール ポリシーを作成するには、まずファイヤーウォール > ポリシー — 基本ページの**カスタム**を選択し、**適用**をクリックします。それからこのページを使用し、カスタム ファイヤーウォール ポリシーを設定します。

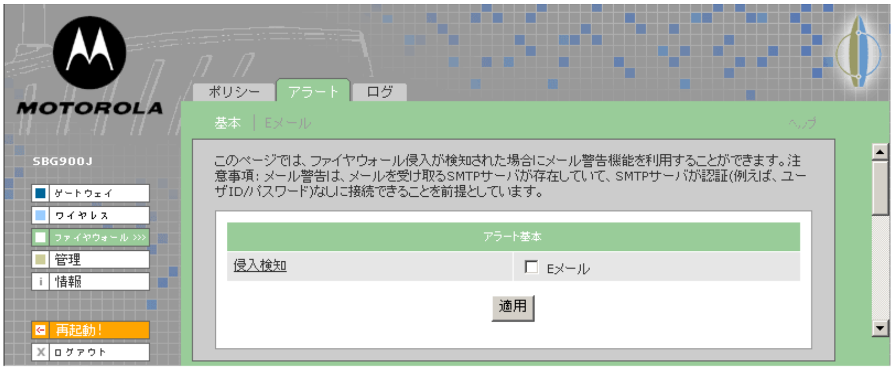
カスタム ポリシーを定義済みファイヤーウォール ポリシー テンプレートを基礎として作成する場合、**ポリシー テンプレート**フィールドで高、中または低を選択し、**ポリシー テンプレートの適用**をクリックします。

ファイヤーウォール > ポリシー— 詳細ページのフィールド

フィールド	説明
新しいフィルタの入力	*詳しい方は*、カスタム ファイヤーウォール フィルタを一つまたはそれ以上設定するためにこれらのフィールドを使用してください。
ポート ID	フィルタを行うプロトコル名を入力します。
有効	ポートのファイヤーウォール ポリシーのフィルタリングを有効にする場合、このボックスを選択します。
許可するプロトコル	ドロップダウン リストから許可するプロトコルを選択します。
ポート範囲（から : まで）	ポート範囲を設定します。プロトコルが必要とするすべてのポートが含まれていなければなりません。
プロトコル番号	許可する IP パケットのプロトコル番号を設定します。
インバウンド許可	インターネットからお使いの LAN へ、インバウンドパケットが通過できるポートを指定することができます。
アウトバウンド許可	インターネットからお使いの LAN へ、アウトバウンド パケットが通過できるポートを指定することができます。ステートフル インスペクションはアウトバウンド セッションのための適切な応答を確認します。
追加	新しいフィルタを追加する場合にクリックします。ファイヤーウォール ポリシー表に表示されます。
ファイヤーウォール ポリシー表	カスタマイズされたファイヤーウォール フィルタの一覧が表示されます。
有効	ポートのファイヤーウォール ポリシーのフィルタリングを有効にする場合、このボックスを選択します。
削除	フィルタを削除する場合に、削除ボックスを選択します。
適用	変更を適用する場合にクリックします。
ポリシー テンプレート	高、中または低の基礎となる、定義済みファイヤーウォール テンプレートをこのドロップダウン リストから選択することができます。これらのテンプレートについては、「ファイヤーウォール ポリシーの設定」で記載しています。
ポリシー テンプレートの適用	選択したポリシー テンプレートを適用し、カスタマイズをキャンセルする場合にクリックします。

ファイヤーウォール > アラート — 基本ページ

ファイヤーウォールへの侵入検知イベントに対するアラート方法を設定するために、このページを使用することができます。

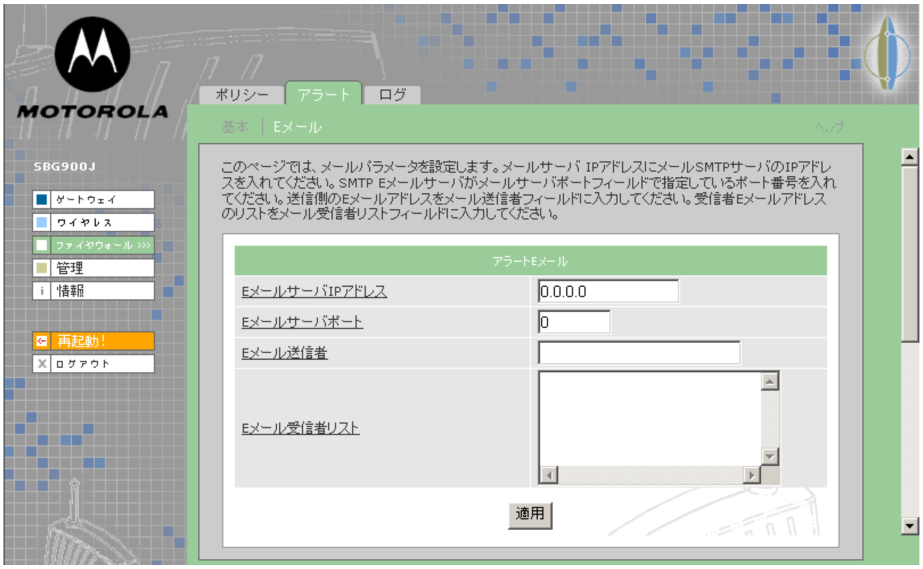


ファイヤーウォール > アラート — 基本ページのフィールド

フィールドまたはボタン	説明
侵入探知	SMTP E メールを通してアラートすべき E メールの選別を行います。E メールを受信するには、ユーザー名またはパスワードなどの認証を必要としない SMTP サーバーが必要となります。
適用	変更を適用する場合にクリックします。

ファイヤーウォール > アラート — E メールページ

このページを使用して、E メールアラートパラメータを設定することができます。



ファイヤーウォール > アラート — E メールページのフィールド

フィールドまたはボタン	説明
E メール サーバー IP アドレス	点区切り 10 進数形式で、E メール サーバーの IP アドレスを設定します。
E メール サーバー ポート	E メール サーバーのポート番号を設定します。
E メール送信者	E メールの送信者アドレスを設定します。
E メール受信者リスト	SBG900J ファイヤーウォールからアラートを受け取る E メールアドレスのリストを設定します。
適用	変更を適用する場合にクリックします。

ファイヤーウォール > ログページ

このページを使用して、どのファイヤーウォールのイベントをログ記録するかを設定することができます。

ファイヤーウォール > ログページのフィールド

フィールドまたはボタン	説明
セッション ログの有効化	SBG900J ファイヤーウォールによって許可されたプライベート LAN からの各データセッションをログへ記録するには、このボックスを選択します。通常、セッション ログには正常なデータ トラフィックの履歴が記録されています。ログには以下の理由でファイヤーウォールが終了したセッションの開始の一覧も表示されます。 • ポリシーが変更された • 進入または攻撃があったと判断された セッションログを表示するには、**セッション**をクリックします。
ブロッキング ログの有効化	SBG900J ファイヤーウォールが以下を行う場合、インバウンドおよびアウトバウンド パケットについてログに記録するには、このボックスを選択します。 • アクティブ ポリシーによって明示的に許可されていないプロトコルおよび / またはポートを使用するため、通過を許可しない場合 • セッションまたは再編成タイムアウトのため、不正であると決定した場合 ブロッキング ログを表示するには、**ブロッキング**をクリックします。
侵入ログの有効化	SBG900J ファイヤーウォールが検出・停止する一般的な侵入方法を使用した攻撃をログ記録する場合にこのボックスを選択します。 侵入ログを表示するには、**侵入**をクリックします。
適用	変更を適用する場合にクリックします。

ファイヤーウォールを有効にした場合、必ずブラックリスト ログが生成されます。ファイヤーウォールがアクティビティ ポリシーに反していると判断した IP アドレスはすべてブラックリスト ログに追加されます。ブラックリスト ログを表示するには、**ブラックリスト**をクリックします。ファイヤーウォールはブラックリストに載っている IP アドレスへの、または IP アドレスからのすべてのトラフィックを 24 時間または SBG900J を再起動するまで、またはファイヤーウォール > ログ — ブラックリスト**消去**をクリックして手動でブラックリストを消去するまで、ブロックします。

ゲートウェイの設定

本セクションには SBG900J 設定プログラムのゲートウェイ設定ページについて記載されています。

- ゲートウェイの有効化
- ゲートウェイ > ステータスページ
- ゲートウェイ > WAN ページ
- ゲートウェイ > LAN — NAT 設定ページ
- ゲートウェイ > LAN — DHCP サーバ設定ページ
- ゲートウェイ > LAN — DHCP リースページ
- ゲートウェイ > ポート フォワーディング— ステータスページ
- ゲートウェイ > ポート フォワーディング— 設定ページ
- ゲートウェイ > ポートトリガー 定義済みページ
- ゲートウェイ > ポートトリガー カスタムページ
- ゲートウェイ > ログページ

フィールドを変更し適用をクリックした後、変更を有効にするために再起動しなければならないことの警告が表示さされます。再起動には約 10 ～ 15 秒かかります。再起動後、もう一度ログインする必要があります。

ゲートウェイの有効化

SBG900J のゲートウェイ機能を使用する場合には、まず最初にゲートウェイの設定を有効にする必要があります。有効にするには：

1 SBG900J 設定プログラムの左パネルで、管理をクリックし、管理－詳細ページを表示します。

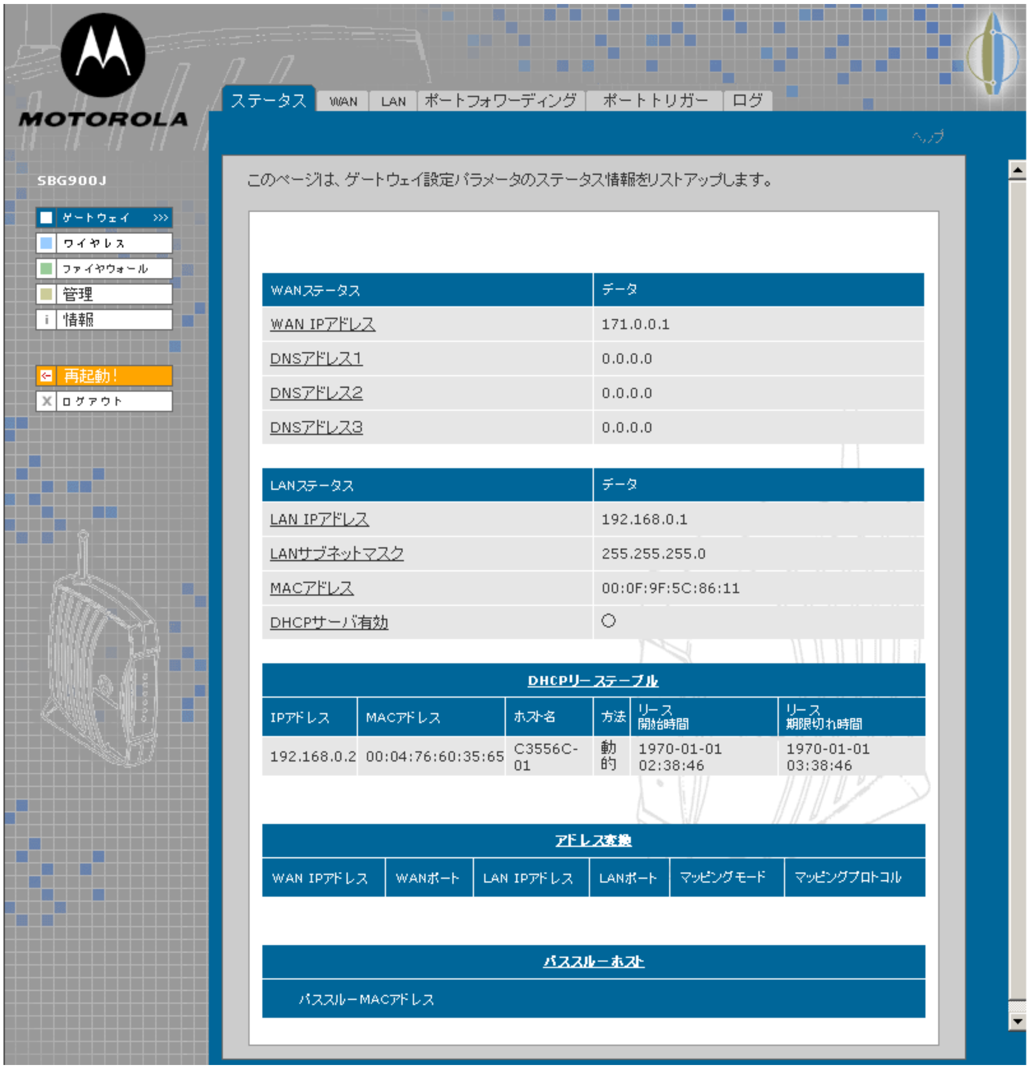
2 ゲートウェイモードの使用を選択します。

3 適用をクリックし、SBG900J 設定プログラムの左パネルで再起動をクリックします。

再起動後、変更が適用がされます。

ゲートウェイ > ステータスページ

このページにはゲートウェイのステータスに関する情報が表示されます。



これらのフィールドには他のゲートウェイページで設定された項目が表示されます。フィールドの説明については、各タブのフィールドについて記載されている以下のサブセクションを参照してください。

ゲートウェイ > WAN ページ

このページを使用して、外部（公衆）広域通信網 (WAN) インターフェースを設定することができます。

ゲートウェイ > WAN ページのフィールド

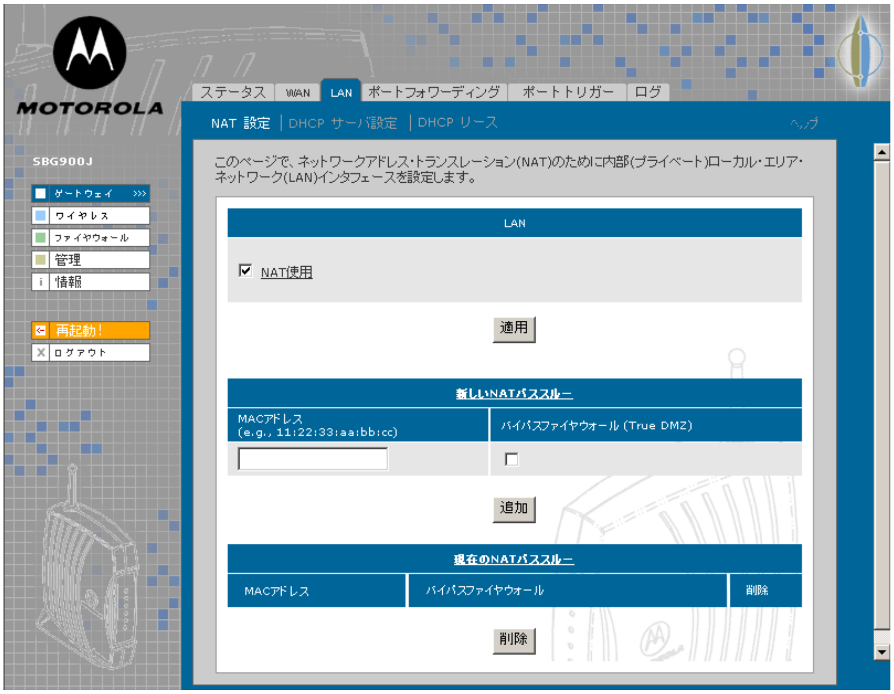
フィールド	説明
ホスト名	ケーブル プロバイダーのネットワークにアクセスするためにホスト名が必要な場合は、このフィールドにプロバイダーから提供された*ホスト名*を入力します。デフォルトでは空欄になっています。
DHCP クライアント有効化（動的 IP アドレス取得）	DHCP クライアント有効化を選択した場合、SBG900J は自動的に外部 IP アドレス、サブネットマスク、ドメイン名、DNS サーバーを取得します。 ケーブル プロバイダーの DHCP サーバーが自動的にパブリック IP アドレスを割り当てる場合、DHCP クライアント有効化を選択します。DHCP クライアント有効化はデフォルトで選択されています。
DHCP クライアント（固定 IP アドレス使用）	ケーブル プロバイダーが DHCP を使用して自動的に外部 IP アドレスを提供しない場合 : • ケーブル プロバイダーは固定 IP アドレス、固定 IP サブネットマスク、WAN デフォルトゲートウェイ IP アドレス、1 ～ 3 つの DNS IP アドレスを提供する必要があります。 • DHCP クライアントの無効化を選択し、各フィールドに固定 IP アドレス、サブネットマスク、WAN デフォルトゲートウェイ、DNS サーバーおよびドメイン名（必要があれば）を入力する必要があります。 DHCP クライアントの無効化はデフォルトでは選択されていません。
固定 IP アドレス	DHCP クライアントの無効化が選択されている場合、ケーブル プロバイダーによって提供される*固定 IP アドレス*を、dotted-decimal（点区切り 10 進数）形式で入力します。デフォルトでは空欄になっています。
固定 IP サブネットマスク	DHCP クライアントの無効化が選択されている場合、固定 IP アドレスと関連した*サブネット マスク*を点区切り 10 進数形式で入力します。デフォルトでは空欄になっています。

ゲートウェイ > WAN ページのフィールド (続き)

フィールド	説明
WAN デフォルトゲートウェイ	ケーブル プロバイダーからの固定 IP アドレスを使用する場合、WAN 上の SBG900J のデフォルトゲートウェイ *IP アドレス*を点区切り 10 進数形式で入力します。
DNS IP アドレス 1 **DNS IP アドレス 2** **DNS IP アドレス 3**	ケーブル プロバイダーの DNS サーバーはホスト名によって IP アドレスの照会を行います。ケーブル プロバイダーが自動的に DHCP サーバーから DNS アドレスを割り当てない場合、点区切り 10 進数形式でこれらのフィールドを入力するため、プロバイダーから少なくとも一つの DNS サーバー IP アドレスを提供されなければなりません。デフォルトでは空欄になっています。
TCP セッション待ちタイムアウト	TCP セッションがタイムアウトであると想定するまでの最大待機時間を秒数で設定します。デフォルトは 86400 秒です。
UDP セッション待ちタイムアウト	UDP セッションがタイムアウトであると想定するまでの最大待機時間を秒数で設定します。デフォルトは 300 秒（5 分）です。
ICMP セッション待ちタイムアウト	ICMP セッションがタイムアウトであると想定するまでの最大待機時間を秒数で設定します。デフォルトは 300 秒（5 分）です。
適用	変更を適用する場合にクリックします。

ゲートウェイ > LAN — NAT 設定ページ

このページを使用して、NAT を有効にし、クライアントを現在の NAT パススルーリストへ追加することができます。



ゲートウェイ > LAN — NAT 設定ページのフィールド

フィールドまたはボタン	説明
LAN	
NAT 有効化	有効になっている場合、ケーブル プロバイダーによって割り当てられた単一 HFC IP アドレス（外部 IP アドレス）は SBG900J LAN 上の多くの内部 IP アドレスへマップされます。
適用	変更を適用する場合にクリックします。SBG900J を再起動する必要があります。
新しい NAT パススルー	クライアントの MAC アドレスを使用して、NAT の対象にはならないパススルー クライアントとして最大 32 台のコンピュータを指定します。*この機能を使用できるようにするには、ケーブル オペレータが追加の外部 IP アドレスを提供する必要があります。*
MAC アドレス	パススルー クライアント MAC アドレスを入力します。16 進数形式で入力します。
バイパスファイヤーウォール (True DMZ)	NAT パススルー コンピュータを DMZ クライアントとして設定する場合に、このボックスを選択します。*DMZ クライアントはインターネット ハッカーに対し完全に開放されているため、この設定を使用する場合は特に注意が必要です。*
追加	現在の NAT パススルーリストへ MAC アドレスを追加する際にクリックします。
現在の NAT パススルー	NAT パススルー用に設定されている LAN 上のコンピュータのリストを表示します。
削除	NAT パススルーリストから MAC アドレスを削除する際にクリックします。

ゲートウェイ > LAN — DHCP サーバ設定ページ

経験豊富なネットワーク管理者のみが、このページを使用して DHCP サーバーの詳細設定を行うべきです。

注意！

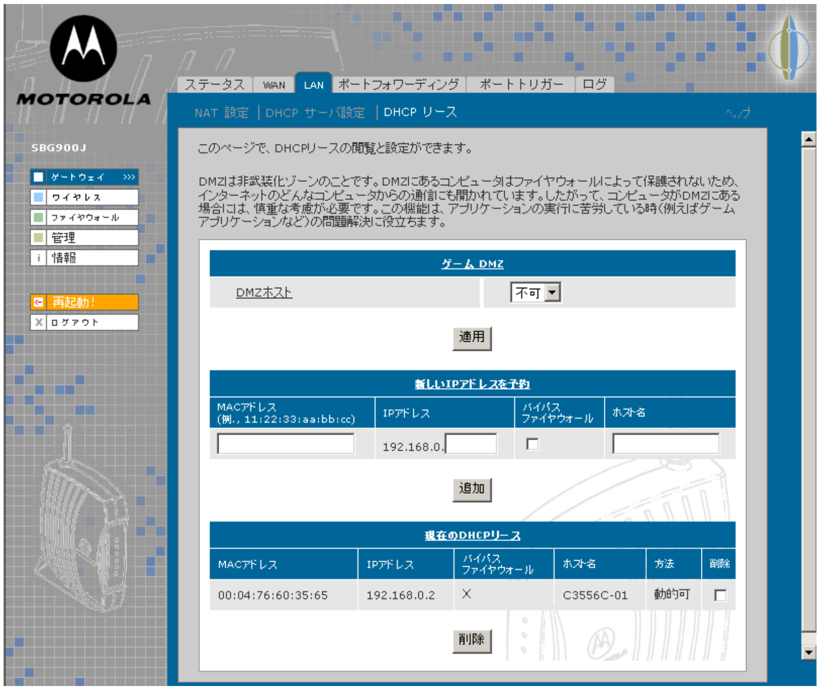
IP アドレス、サブネット、DHCP に関する詳しい知識のある経験豊富なネットワーク管理者以外、これらの設定を変更しないでください。

ゲートウェイ > LAN — DHCP サーバ設定ページのフィールド

フィールド	説明
LAN IP アドレス	プライベート LAN の SBG900J の *IP アドレス*を入力することができます。デフォルト値は 192.168.0.1 です。
LAN IP サブネットマスク	点区切り 10 進数形式のサブネットマスクを表示します。デフォルト値は 255.255.255.0 です。
開始 IP アドレス	SBG900J DHCP サーバーによってクライアントに割り当てられる開始 *IP アドレス*を点区切り 10 進数形式で入力します。デフォルト値は 192.168.0.2 です。
DHCP ユーザー数	内部 IP アドレスを割り当てるため、SBG900J DHCP サーバーのクライアント数を設定します。利用できるクライアント アドレス数は 253 個です。デフォルト値は 253 です。
DHCP サーバーリース時間	SBG900J DHCP サーバーが IP アドレスをクライアントに貸し出す（リースする）*時間*を秒数で設定します。デフォルトは 3600 秒（60 分）です。
ドメイン名	SBG900J LAN の*ドメイン名*を設定します。デフォルトでは空欄になっています。
TTL 値	アウトバウンド パケットの *TTL（中継限界数）*を設定します。デフォルト値は 64 です。
インターフェース最大伝送ユニット	SBG900J LAN の MTU をバイト数で設定します。最小値は 68 バイトです。デフォルト値は”０”です。”0”の時は、この設定は無効です。
適用	変更を適用する場合にクリックします。SBG900J を再起動する必要があります。

ゲートウェイ > LAN — DHCP リースページ

このページを使用して、DHCP リースを設定します。



ゲートウェイ > LAN — DHCP リースページのフィールド

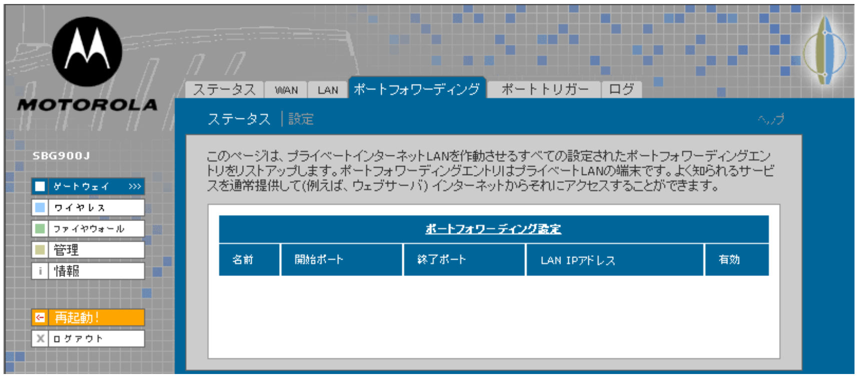
フィールド	説明
ゲーム DMZ	
ゲーム DMZ の有効化	選択したコンピュータまたはゲーム機器をゲーム DMZ ホストとして指定する場合、このボックスを選択します。これは、ある種のアプリケーション（一般的にゲーム アプリケーション）が実行できない場合に便利です。
ゲーム DMZ ホスト	ゲーム DMZ ホストは、デフォルト DMZ ホストそして指定された、予約 IP アドレスを持つコンピュータです。一度に一つのゲーム DMZ ホストしかアクティブにできません。*ゲーム DMZ ホストはファイヤーウォールによって保護されていません。インターネット上のどのコンピュータからでも、通信またはハッキングできます。*DMZ に配置するコンピュータを設定する前に、十分考慮してください。 NAT パススルー ホストではなくゲーム DMZ ホストを使用することの利点は、ゲーム DMZ ホストは NAT パススルー ホストと異なり、外部 IP アドレスを必要としない点にあります。アプリケーションが外部 IP アドレスを要求した場合、ゲートウェイ > LAN — NAT 設定ページでコンピュータを NAT パススルー用に設定します。
新しい IP アドレスの予約	SBG900J DHCP サーバーによって割り当てられた最大 32 個の IP アドレスを特定の LAN クライアント用に予約することができます。例えば、常に同じ内部 IP アドレスを確実に受け取るよう、内部 FTP サーバーまたはゲーム DMZ デバイス用に IP アドレスを予約することができます。
MAC アドレス	予約 IP アドレスが必要な DHCP クライアントの MAC アドレスを入力します。16 進数形式で入力します。
IP Address（IP アドレス）	特定の MAC アドレスを持つ LAN クライアント用の予約 IP アドレスのホスト部分を設定します。LAN クライアントが IP アドレスを要求した時、SBG900J DHCP サーバーはクライアントへこの IP アドレスを割り当てます。
ホスト名	ISP のネットワークにホスト名が必要な場合、ホスト名フィールドへ提供されたホスト名を入力します。

ゲートウェイ > LAN — DHCP リースページのフィールド (続き)

フィールド	説明
追加	新しい IP アドレスを予約する場合、追加をクリックします。
現在予約されている IP アドレス	予約 IP アドレスを持つすべての DHCP クライアントを表示します。
MAC アドレス	クライアント MAC アドレスを表示します。
IP アドレス	予約 IP アドレスを表示します。
バイパスファイヤウォール	予約した ＩＰ アドレスをバイパスする時に、このボックスを選択します。
ホスト名	ホスト名を表示します。
方法	動的および静的リース状態を表示します。このフィールドの動的または静的リース状態を追加または削除します。
削除	削除する予約 IP アドレスを指定するには、このボックスを選択します。
削除	削除ボックスで指定されたクライアントの予約 IP アドレスを削除する際に、このボタンをクリックします。

ゲートウェイ > ポート フォワーディング— ステータスページ

このページを使用して、SBG900J LAN の設定されたポート フォワーディング入力項目を表示します。ゲートウェイ > ポート フォワーディング— 設定ページのフィールドと同じです。



ゲートウェイ > ポート フォワーディング— 設定ページ

このページを使用して、最大 32 の仮想サーバーを設定します。

ゲートウェイ > ポート フォワーディング— 設定ページのフィールド

フィールド	説明
新しいポートフォワーディングエントリ追加	最大 32 のポートフォワーディングができます。カスタムを選択した場合、名前、開始ポート、終了ポート、および LAN IP アドレスを設定しなければなりません。
テンプレート	カスタムを選択した場合、名前、開始ポート、終了ポート、および LAN IP アドレスを設定しなければなりません。 HTTP または FTP などの定義済みテンプレートを選択した場合、名前、開始ポート、終了ポートの値は既に設定されています。LAN IP アドレスのみ入力する必要があり、必要がある場合のみ、デフォルト値を変更します。
名前	カスタム仮想サーバーの固有識別名を入力します。一般的に、プロトコルを固有識別名として使用します（例えば「ftp」）。
開始ポート	LAN 内部インターフェース ポートまたはポート範囲の開始を設定します。インバウンド インターネット接続要求はこのポートへ固定的にマップされます。以下は一般的なアプリケーションで使用されるポートです。 • FTP 20, 21 • HTTP 80 • NTP 123 • Secure Shell 22 • SMTP E メール 25 • Telnet 23
終了ポート	ポートの範囲が必要な場合、ポート範囲の終了値を設定します。
LAN IP アドレス	ポート フォワーディング ページ用に内部 LAN IP アドレスを設定します。プライベート LAN 上で定義した任意のポート フォワーディング項目へアクセスするためには、インターネット ユーザーは外部 IP アドレスを知っている必要があります。

ゲートウェイ > ポート フォワーディング— 設定ページのフィールド (続き)

フィールド	説明
有効	NAT 経由でアクセスするためポート フォワーディング項目を有効にするには、このボックスを選択します。
追加	ポート フォワーディングリストへ仮想サーバーを追加する際にクリックします。
ポート フォワーディング	設定されたカスタム仮想サーバーを表示します。

ゲートウェイ > ポートトリガ— 定義済みページ

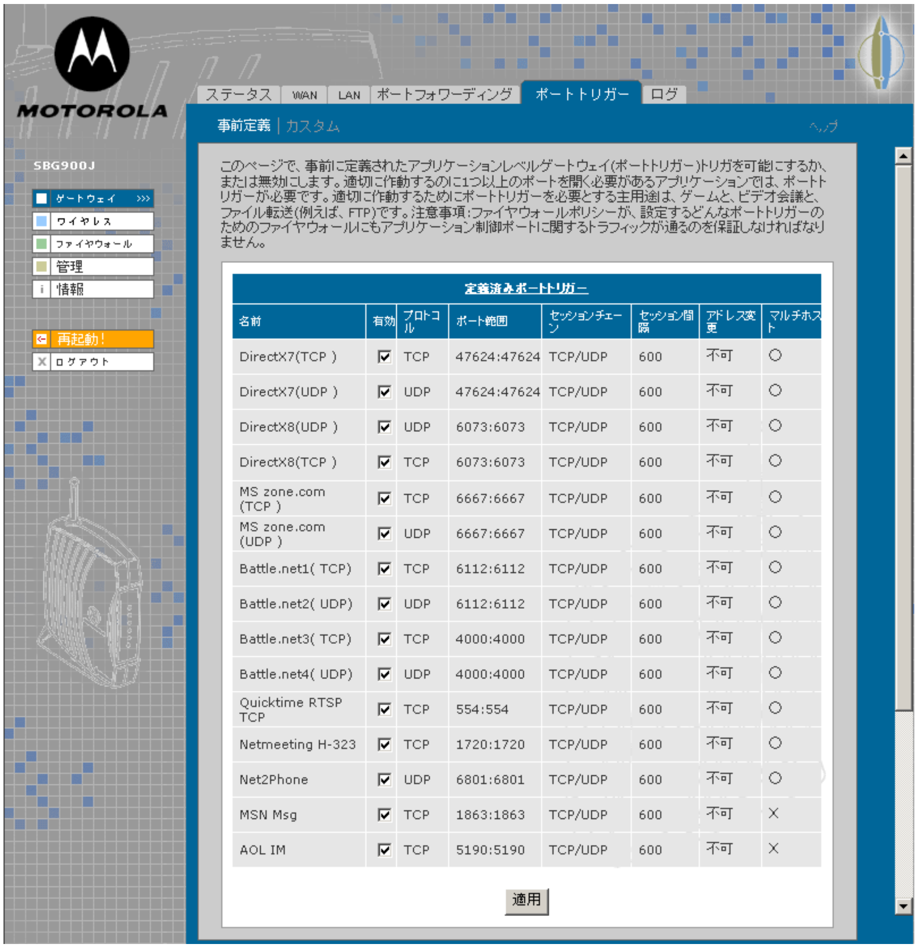
インターネットへアクセスする PC アプリケーションを実行する場合、アプリケーションはインターネット上のコンピュータと通信を行います。特にゲームなどのアプリケーションによっては、インターネット上のコンピュータもまた、お使いの PC との通信を行います。NAT は一般的にこれらの受信接続を許可しないため、SBG900J はポート トリガリングをサポートしています。

SBG900J では、共通アプリケーション用のポート トリガリングが既に設定されています。必要があれば、追加ポート トリガを設定することができます。アプリケーション用ポート トリガの設定には以下が必要です。

- アプリケーション トランスポート プロトコル — TCP または UDP
- アプリケーション ポート番号

その他のパラメータについては、デフォルト値を使用することができます。

一度に SBG900J に接続された一台のコンピュータのみ、ポート トリガリングを必要とするアプリケーションを使用することができます。このページを使用して、定義済みポート トリガリングを表示することができます。

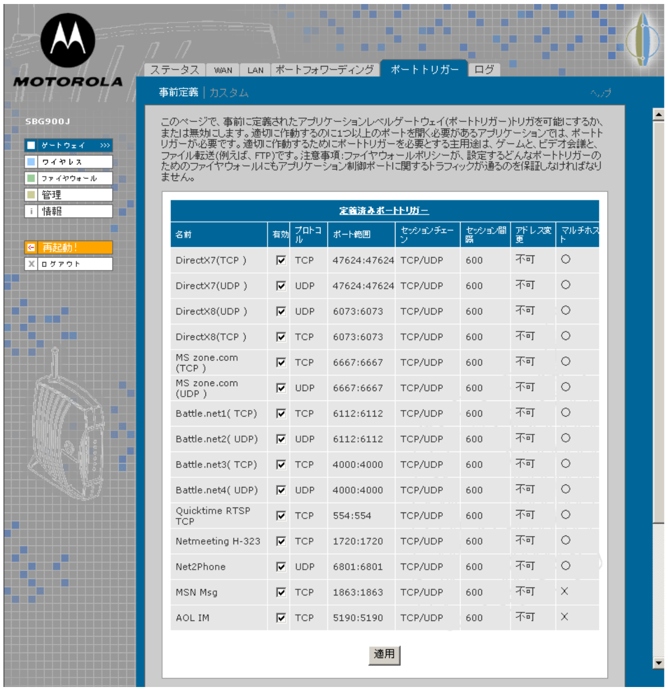


ゲートウェイ > ポートトリガ— 定義済みページのフィールド

フィールド	説明
名前	ポート トリガの固有名を表示します。一般的に、プロトコル名が使用されます。
ポートトリガーを有効にする	定義済みアプリケーション用にポート トリガを起動するには、このボックスを選択します。
プロトコル	ポート トリガのアプリケーション トランスポート プロトコル — TCP または UDP を表示します。
ポート範囲	ポート トリガのポート範囲（から : まで）を表示します。
セッションチェーン	ポート トリガ — 無効、TCP または TCP/UDP のセッションポート チェーンの選択肢を表示します。
セッション間隔	ポート トリガ用に設定されたセッション間隔を表示します。
アドレス変換	ポート トリガ用のアドレス置き換え方法を表示します。
マルチホスト	ポート トリガ用のマルチ ホストの選択肢を表示します。

ゲートウェイ > ポートトリガー カスタムページ

このページを使用して、カスタム ポート トリガリングを作成します。



ゲートウェイ > ポートトリガー カスタムページのフィールド

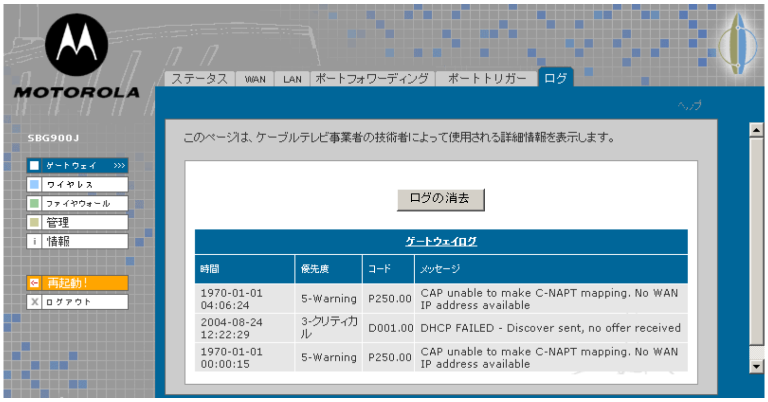
フィールド	説明
新しい特別アプリケーションの追加	
名前	ポート トリガの固有名を入力します。通常プロトコル名を使用します。
有効	カスタム ポート トリガリングを有効にする場合は、このボックスを選択します。
プロトコル	ポート トリガのトランスポート プロトコル — TCP または UDP を設定します。
ポート範囲 から : まで	ポート トリガのポート範囲を設定します。左のフィールドに範囲の開始値を入力し、右のフィールドに終了値を入力します。
セッションチェーン	適切に操作を行うために、アプリケーションが一つ以上のポートを異なる範囲で開く必要がある場合、セッション チェーンを有効にします。選択肢として、Disable（無効）、TCP または TCP/UDP があります。
セッション間隔	アプリケーションのセッション間隔を設定します。 • ポート トリガがセッション間隔内でポート範囲のトラフィックを検出した場合、それは初期セッションと関連があるとみなされます。 • ポート トリガがセッション間隔の期限切れ後にポート範囲のトラフィックを検出した場合、それは新しい、独自のセッションであるとみなされます。
アドレス置き換え	アプリケーション用のアドレス置き換え方法を設定します。
マルチホスト	アプリケーションにとって適切である場合選択します。

ゲートウェイ > ポートトリガ— カスタムページのフィールド (続き)

フィールド	説明
追加	ポートトリガテーブルへポート トリガを追加する際にクリックします。
ポートトリガテーブル	定義されたすべてのポート トリガとそのパラメータの一覧を表示します。

ゲートウェイ > ログページ

このページを使用して、ゲートウェイの詳細情報を表示します。



ゲートウェイ > LOG（ログ）ページのフィールド

フィールド	説明
時間	日時のフォーマットは yyyy-mm-dd hh:mm:ss です。
優先順位	メッセージの重要性を示します。
コード	メッセージに関連する文字コード。
メッセージ	イベントの説明。

ワイヤレス LAN を設定する

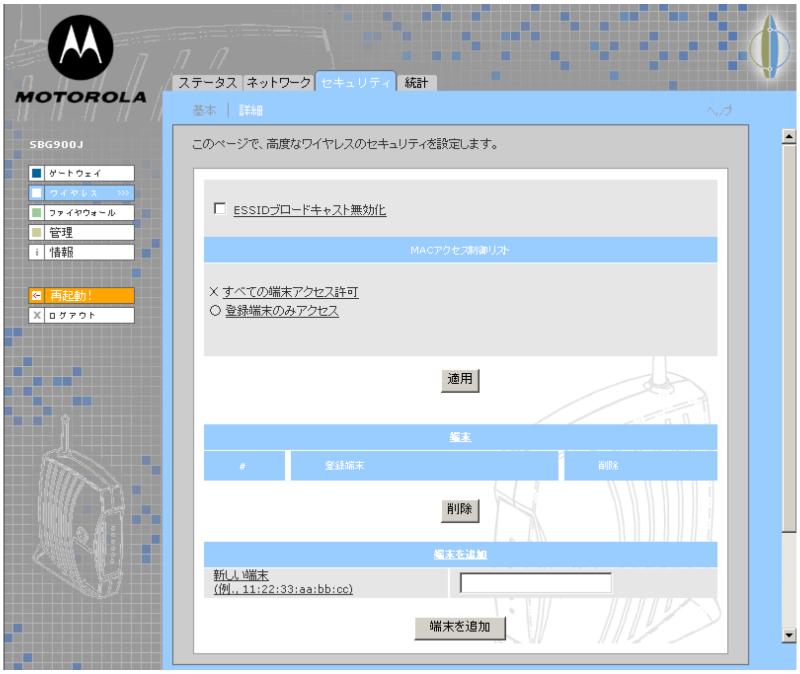
SBG900J をワイヤレス LAN のアクセスポイントとして使用する場合には、まず最初に使用する無線 LAN カードの MAC アドレスを登録する必要があります。

無線ＬＡＮカードの MAC アドレスを登録するには：

1 SBG900J 設定プログラムの左パネルで、ワイヤレスをクリックし、ワイヤレスーセキュリティページ内の詳細を表示します。

2 新しいステーションを追加の新しいステーション欄にワイヤレスクライアントの MAC アドレスを形式として××：××：××：××：××：××にて入力します

3 ステーションの追加をクリックすると登録されます。MAC アクセス制御リストには 1 ～ 32 のクライアントの登録が可能です。



注意！

WLAN 上の不正盗聴または不正アクセスを防ぐため、ワイヤレス セキュリティを有効に設定しなければなりません。SBG900J のデフォルト設定では、ワイヤレスデータのセキュリティが提供されていません。WLAN が操作できる状態になったら、ワイヤレス セキュリティを有効にしてください。

SBG900J WLAN のセキュリティを有効にするには、SBG900J 上で以下を行うことができます：

項目	行うこと	設定プログラムでの使用
ワイヤレス送信の暗号化および WLAN アクセスの制限	ワイヤレス LAN 送信の暗号化	ワイヤレス > セキュリティ― 詳細ページ
WLAN への不正侵入を更に防ぐ	ワイヤレス LAN アクセスの制限	ワイヤレス > セキュリティ― 詳細ページ

設定を行うために、少なくとも 1 台のコンピュータを SBG900J イーサネットポートに接続してください。ワイヤレス接続では SBG900J の設定はできません。

「ワイヤレス クライアントを設定する」で記載されている通り、SBG900J LAN へアクセスするには各ワイヤレス クライアントを設定する必要があります。

注意！

ESSID、WPA または WEP パスフレーズまたは WEP キーをお使いの WLAN への使用を許可されていない人物に教えないでください。

すべてのワイヤレス設定フィールドの説明は、「SBG900J 設定プログラムのワイヤレスページ」を参照してください。

ワイヤレスセキュリティを向上する基本的な手順として、ワイヤレスコンポーネントを窓から離れた場所に置くことがあげられます。

ワイヤレス LAN 送信の暗号化

WLAN 上における送信データの不正盗聴を防ぐため、ワイヤレス送信を暗号化しなければなりません。

送信データを暗号化するには、ワイヤレス > セキュリティー 詳細ページを使用します。以下から一つ選択します。

SBG900J で行う設定	各ワイヤレス クライアントで必要なこと
お使いのワイヤレス クライアントすべてが WPA:Wi-Fi Protected Access をサポートしている場合、SBG900J で WPA を設定することを推奨します。	ローカル WPA-PSK のパスフレーズを使用する場合、SBG900J と同じパスフレーズを各ワイヤレスクライアント上で設定しなければなりません。通常ローカルパスフレーズを使用します。 RADIUS サーバーの設定には専門的な知識が必要となり、このガイドの範囲外です。詳しくは、お使いのネットワークの管理者へお問い合わせください。
それ以外の場合は、SBG900J で WEP を設定するを行います	各ワイヤレス クライアント上で SBG900J と同一の ＷＥＰ キーを設定しなければなりません。

すべてのクライアントが WPA 暗号化をサポートしている場合、以下の理由で WEP ではなく WPA の使用を推奨します。

- WPA は暗号強度が高く、より安全です
- WPA は、お使いの WLAN に許可されているユーザーのみが確実にログインするよう、認証を提供します
- WPA は設定がより簡単です
- WPA は標準アルゴリズムを使用し、すべての準拠製品がテキスト形式のパスフレーズからキーを生成することができます
- WPA には新しい IEEE 802.11i ワイヤレスネットワーキング標準が組み込まれることになります

新しいワイヤレス LAN では、WPA をサポートするクライアント アダプタをご購入するようお奨めします。WPA の利点について詳しくは、Wi-Fi Protected Access ウェブページである http://www.wifialliance.org/OpenSection/protected_access.asp を参照してください。

SBG900J で WPA を設定する

WPA を有効にし、SBG900J でキーを設定するには、

1 SBG900J 設定プログラムの左パネルで、**ワイヤレス**をクリックします。

2 セキュリティタブをクリックし、ワイヤレス > セキュリティー 基本ページを表示します。

3 セキュリティ モードフィールドで、**WPA** を選択し、**適用**をクリックします。

4 WPA の設定で、**WPA 暗号化**の種類を一つ選択します。*TKIP では動作が遅くなる場合がありますので、クライアントが AES をサポートしている場合は AES を選択してください。*

TKIP TKIP（Temporal Key Integrity Protocol）は一定パケットのキー複合機能、メッセージ完全性チェック (MIC)、初期ベクトル (IV) および再キー生成構造を含むデータ暗号化を提供します。

AES Advanced Encryption Standard（高度暗号化標準規格）は、128 ビットキーを使用したブロック暗号として対称キー暗号を実装しています。すべてのワイヤレス クライアントが AES をサポートしている場合、この設定を使用するよう推奨いたします。

5 **WPA** 認証の種類を選択します :

リモート (Radius)	リモート認証ダイアルインユーザーサービス (RADIUS) サーバーが利用できる場合、このオプションを選択することができます。ステップ 6 へ進みます。RADIUS サーバーは通常大企業などで使用されます。
ローカル (WPA-PSK)	事前共有キー (PSK) ローカル認証を選択した場合、WPA をサポートするすべてのクライアント上のパスフレーズは SBG900J で設定した PSK パスフレーズと一致し、クライアントは SBG900J WLAN へとアクセスすることができます。PSK パスフレーズを設定するには、ステップ 7 へ進みます。ローカルキーは一般的に家庭または小規模オフィスで使用されます。

6 リモート **(RADIUS)** 認証のみの場合、以下を設定します :

Radius ポート	RADIUS サーバーでリモート認証のために使用するポート。使用できる数値は 0 ～ 65535 です。
Radius キー	リモート認証のキー。使用できる文字は 0 ～ 255ASCII 文字です。
Radius サーバーの種類	現在は IPv4 のみです。
Radius サーバー	点区切り 10 進数形式 (xxx.xxx.xxx.xxx) の、RADIUS サーバー IP アドレス。

7 ローカル **(WPA-PSK)** 認証のみでは、以下を設定します。

PSK パスフレーズ	8 ～ 63 ASCII 文字を含む PSK パスワード。各 WLA クライアント上で同一のパスフレーズを設定しなければなりません（「WPA 用にワイヤレス クライアントを設定する」を参照してください)。

8 **保存**をクリックします。

ワイヤレスの初期設定を復元する必要がある場合は、**ワイヤレスデフォルトのリセット**をクリックします。

SBG900J で WEP を設定する

WPA をサポートしていないワイヤレス クライアントのみを使用している場合、WEP（Wired Equivalent Privacy Encryption）を使用します。

注意！

> WEP 暗号を使用する場合、SBG900J アクセス ポイントおよびすべてのワイヤレス クライアント（ステーション）で、同じ WEP キーを設定する必要があります。*WLAN の使用を許可されていない人物へ、WEP キーまたはパスフレーズを教えないでください。*

WEP を有効にし、SBG900J でキーを設定するには、

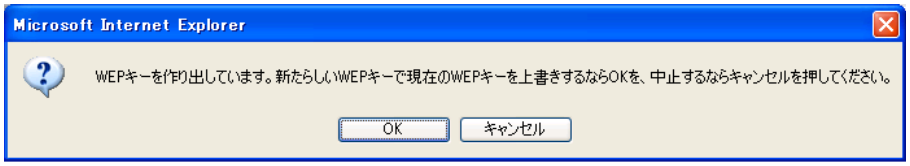
1 SBG900J 設定プログラムの左パネルで、**ワイヤレス**をクリックします。

2 セキュリティタブをクリックし、ワイヤレス > セキュリティ— 基本ページを表示します。

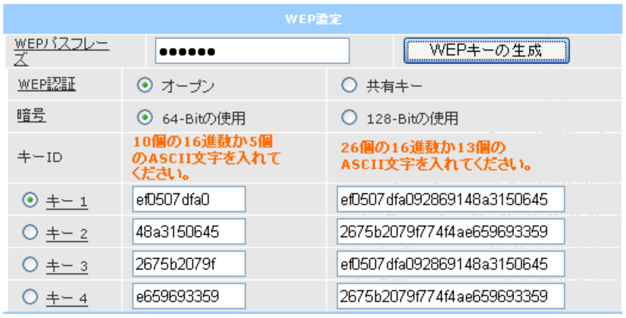
3 セキュリティ モードフィールドで、**WEP** を選択し、**適用**をクリックします。

4 **WEP** パスフレーズフィールドで、8 ～ 31 の ASCII 文字を含む*パスフレーズ*を入力します。プライバシーを考慮し、パスフレーズはドットで表示されます。

5 **WEP キーの生成**をクリックします。以下のようなウィンドウが表示されます。



6 **OK** をクリックします。WEP 設定フィールドは下のように表示されます。



ステップ 7 を行う前に、以下の点を考慮してください：

- すべてのワイヤレス アダプタが 128 ビット暗号化をサポートしている場合、**128 ビットの有効化**を選択することができます。サポートしていない場合は、**64 ビットの有効化**を選択しなければなりません。
- ステップ 7 で指定した生成済み WEP キーを入力する必要がある場合もあります。

7 WEP 設定で、以下の項目を設定します。

WEP 認証

WLAN 上でデータ プライバシーを提供するために、共有キー認証を有効にするかどうかを設定します：

- オープン システム― 任意の WLAN クライアントは認証なく他のクライアントへデータを送信することができます。セキュリティ モードが WEP に設定されている場合 、これがデフォルトです。
- 共有キー― SBG900J は共有キー認証が有効になっているクライアントへのデータまたはクライアントからのデータを認証し、送信します。*この設定を推奨します。*

暗号化

お使いのワイヤレス クライアント アダプタと互換性のある WEP キー長を使用します。以下から一つ選択します。

- 64 ビットの使用― 128 ビット暗号化をサポートしないワイヤレス クライアントをお持ちの場合のみ使用します。
- 128 ビットの使用― より強力な暗号化のため、この設定を推奨します。

キー 1 ～キー 4

アクティブなキー (1 ～ 4) を選択します。アクティブにできるキーは一つのみです。以下を定義するため、ステップ 4 からステップ 6 で記載されている通り、または大文字小文字を区別しない 16 進数の文字である 0 ～ 9 および A ～ F までを入力し、パスフレーズから WEP キーを生成することができます。

- 各 10 文字長の 4 つまでの 64 ビット WEP キー
- 各 26 文字長の 4 つまでの 128 ビット WEP キー

WEP キーは頻繁に変更するよう推奨いたします。WLAN の使用を許可されていない人物へ、WEP キーを教えないでください。

8 **保存**をクリックし、変更を保存します。

ワイヤレスの初期設定を復元する必要がある場合は、**ワイヤレス デフォルトにリセット**をクリックします。

ワイヤレス LAN アクセスの制限

SBG900J ワイヤレスのデフォルト設定により、WLAN へアクセスするためにどのコンピュータでも互換性があるワイヤレス アダプタを持てるようになります。ネットワークを不正侵入から守るため、ワイヤレス > セキュリティー 詳細ページで WLAN へのアクセスを一定のコンピュータ数に制限することができます。

以下の一つまたは両方を設定することができます。

SBG900J で行う設定	各ワイヤレス クライアントで必要なこと
閉鎖ネットワーク操作を有効にするため ESSID（Extended Service Set Identifier）ブロードキャストを無効するよう、SBG900J でワイヤレス ネットワーク名を設定するを行います。	SBG900J と同一の ESSID（ネットワーク名）を設定しなければなりません。
分かっている MAC アドレスを持つワイヤレス クライアントにアクセスを制限するには、SBG900J の MAC アクセス制御リストを設定するを行います。	クライアントでの設定は必要ありません。

SBG900J でワイヤレス ネットワーク名を設定する

SBG900J で ESSID ブロードキャストを無効に設定した場合、SBG900J はネットワーク名 (ESSID) を送信しません。これにより、以下の理由で保護を強化することができます。

- お使いのネットワーク名が設定されているワイヤレス クライアントのみ SBG900J と通信することができます。
- 安全でない WLAN を探している個人による、お使いの WLAN へのアクセスがよりいっそう難しくなります。

閉鎖ネットワーク操作は IEEE802.11b および IEEE802.11g 標準の強化された機能です。

ESSID ブロードキャスト無効化を選択するには、すべての WLAN クライアント（ステーション）に対してワイヤレス クライアントにネットワーク名 (ESSID) を設定するを行わなければなりません。WLAN の使用を許可されていない人物へ、ESSID を教えないでください。

SBG900J で ESSID を設定するには、

1 「SBG900J 設定プログラムの開始」で記載されている通り、SBG900J 設定プログラムを開始します。

2 左のパネルで、**ワイヤレス**をクリックします。

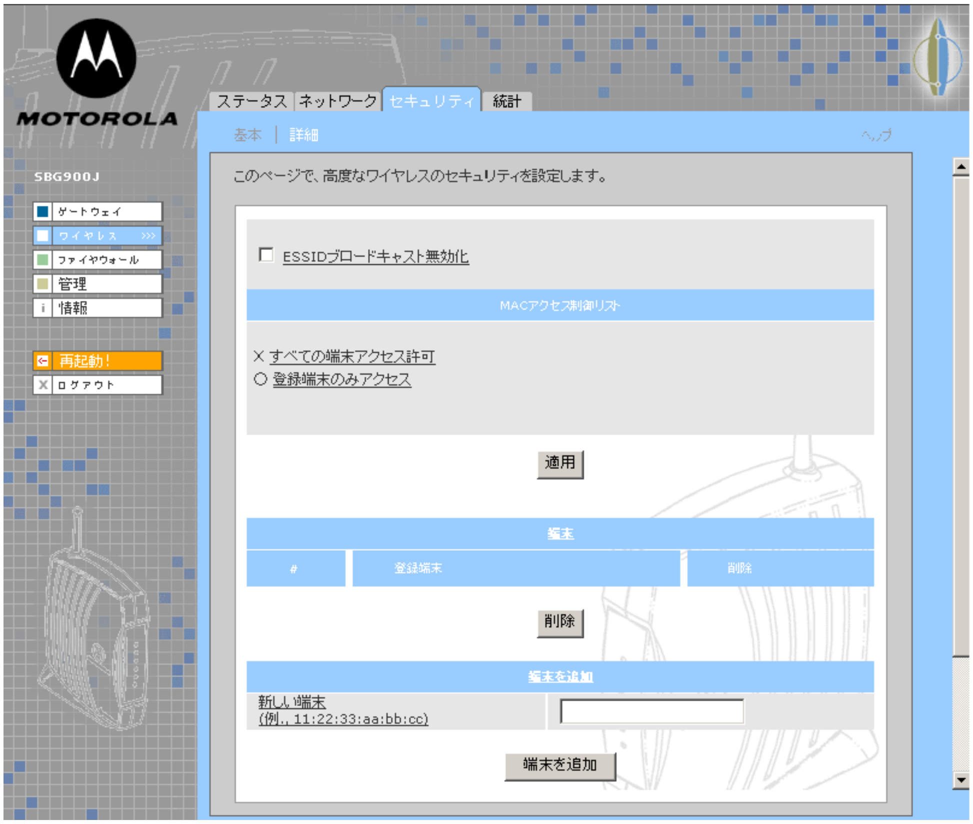
3 **ネットワーク**タブをクリックします。

4 **ESSID** フィールドに、固有*名*を入力します。2 文字から最大 32 文字の、大小文字を区別した英数字が使用できます。デフォルト値は「Motorola」です。*デフォルト ESSID を使用し続けないでください。*

5 **保存**をクリックし、変更を保存します。

6 SBG900J と同じネットワーク名 (ESSID) が設定されたクライアントへの WLAN のアクセスを制限するため、**セキュリティ**タブをクリックします。

7 詳細をクリックし、ワイヤレス > セキュリティー 詳細ページを表示します。



8 SBG900J と同じネットワーク名 (ESSID) が設定されたクライアントへのワイヤレス LAN のアクセスを制限するため、**ESSID ブロードキャスト無効化**を選択します。

9 **適用**をクリックし、変更を保存します。

SBG900J の MAC アクセス制御リストを設定する

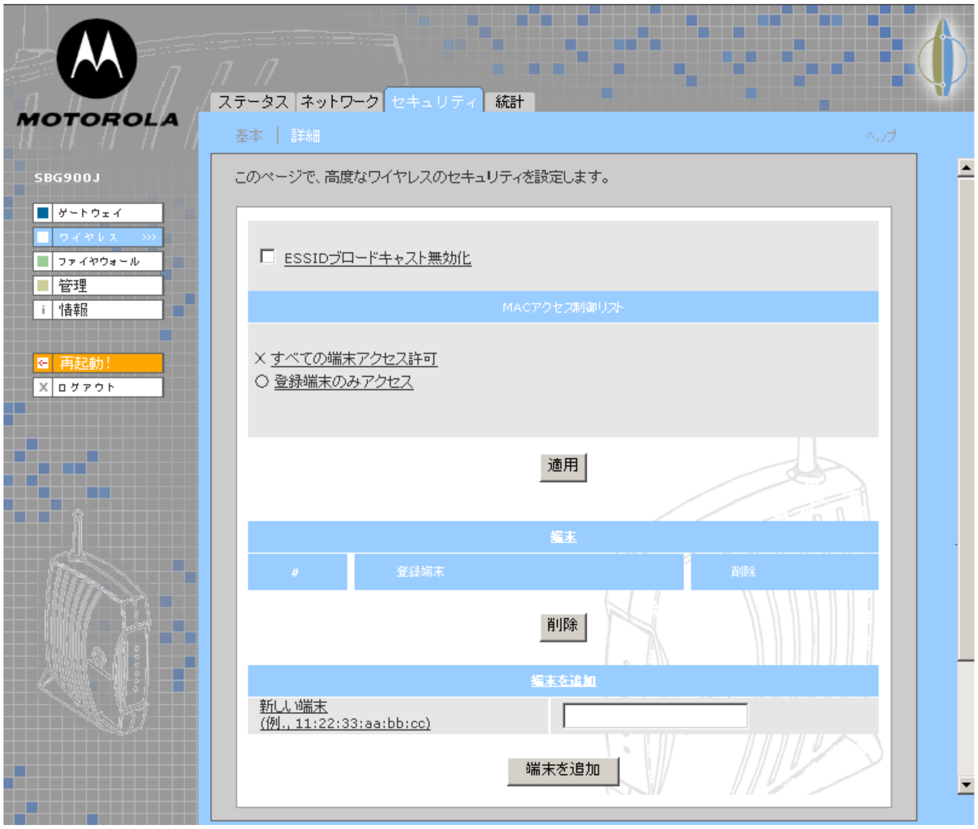
クライアント MAC アドレスに基づき、1 ～ 32 台のワイヤレスクライアントへワイヤレスへのアクセスを制限することができます。

MAC アクセス制御リストを設定するには、

1 SBG900J 設定プログラムの左パネルで、**ワイヤレス**をクリックします。

2 **セキュリティ**タブをクリックします。

3 **詳細**をクリックし、ワイヤレス > セキュリティー 詳細ページを表示します。



4 MAC アクセス制御リスト内にあるシステムへのみワイヤレス アクセスを制限するには、**登録ステーションのみアクセスを許可する**を選択します。本製品はこの設定がディフォルトとなっており、変更はできません。

5 ワイヤレス クライアントを追加するには、**新しい端末**フィールドへ ***xx:xx:xx:xx:xx:xx*** 形式で MAC アドレスを入力し、**端末を追加**をクリックします。

MAC アクセス制御リストへは、最大 32 台のワイヤレス クライアントを追加することができます。

ワイヤレス クライアントを設定する

各ワイヤレス クライアント コンピュータ（ステーション）で、ワイヤレス アダプタを、アダプタ付属の指示書に従い、インストールします。以下が行われていることを確認してください。

1 クライアントの CD-ROM ドライブにアダプタ用の CD-ROM が挿入されていること。

2 CD からデバイス ソフトウェアをインストールすること。

3 PCMCIA または PCI スロットにアダプタが挿入されていること、または USB ポートへ接続されていること。

IP アドレスを自動的に取得するために、アダプタを設定します。

インターネットをサーフするためにワイヤレス クライアント コンピュータを使用するには、以下を行う必要がある場合があります。

以下を行った場合	各クライアントで行う必要のあること
SBG900J で WPA を設定する	WPA 用にワイヤレス クライアントを設定する
SBG900J で WEP を設定する	WEP 用にワイヤレス クライアントを設定する
SBG900J でワイヤレス ネットワーク名を設定する	ワイヤレス クライアントにネットワーク名 (ESSID) を設定する
SBG900J の MAC アクセス制御リストを設定する	クライアントでの設定の必要はありません

WPA 用にワイヤレス クライアントを設定する

WPA を有効にし、PSK パスフレーズを SBG900J で WPA を設定するで設定した場合、同じパスフレーズ（キー）を各ワイヤレス クライアントで設定する必要があります。以下の場合、SBG900J は認証を行うことができません。

- SBG900J では WPA が有効になっているが、クライアント上では有効になっていない場合
- クライアント パスフレーズが SBG900J PSK パスフレーズと一致しない場合

Windows XP での WPA サポートについて詳しくは、以下をご覧ください。

家庭用ネットワークのための WPA ワイヤレス セキュリティ	http://www.microsoft.com/WindowsXP/expertzone/columns/bowman/03july28.asp
Windows XP での WPA ワイヤレス セキュリティ アップデートの概要	http://support.microsoft.com/?kbid=815485

http://www.microsoft.com/downloads/details.aspx?FamilyId=009D8425-CE2B-47A4-ABEC-274845DC9E91&displaylang=en から Microsoft Windows XP の WPA 用サポートパッチをダウンロードすることができます。

注意！

WLAN の使用を許可されていない人物へ、PSK パスフレーズを教えないでください。

WEP 用にワイヤレス クライアントを設定する

WEP を有効にし、SBG900J で WEP を設定するでキーを設定した場合、同じ WEP キーを各ワイヤレス クライアントで設定する必要があります。以下の場合、SBG900J は認証を行うことができません。

- SBG900J では共有キー認証が有効になっているが、クライアント上では有効になっていない場合
- クライアント WEP キーが SBG900J WEP キーと一致しない場合

すべてのワイヤレスアダプタでは、SBG900J で生成された 64 ビットまたは 128 ビットの WEP キーを入力しなければなりません。

注意！

WLAN の使用を許可されていない人物へ、WEP キーを教えないでください。

ワイヤレス クライアントにネットワーク名 (ESSID) を設定する

近隣でご使用のワイヤレス LAN と区別するため、お使いの WLAN に固有のネットワーク名（ネットワーク識別子または ESSID と呼ばれます）を指定することができます。ネットワーク識別子、ネットワーク名または ESSID を尋ねるプロンプトが表示されたら、SBG900J 設定プログラム内のワイヤレス > ネットワークページにある ESSID フィールドへ、*名前*を入力します。詳しくは「SBG900J でワイヤレス ネットワーク名を設定する」を参照してください。

ネットワーク名を指定した後、多くのワイヤレスカードまたはアダプタは自動的に SBG900J などのアクセスポイントをスキャンし、適切なチャンネルとデータ転送速度をスキャンします。お使いのカードでアクセス ポイントのスキャン開始を手動で行わなければならない場合、カードに付属している文書内の指示に従ってください。

WLAN の使用を許可されていない人物へ、ESSID を教えないでください。

SBG900J 設定プログラムのワイヤレスページ

Wireless（ワイヤレス）ページを使用して、ワイヤレス インターフェースを制御および監視することができます。

- ワイヤレス > ステータスページ
- ワイヤレス > ネットワークページ
- ワイヤレス > セキュリティー 詳細ページ
- ワイヤレス > セキュリティー 詳細ページ
- ワイヤレス > 統計ページ

フィールドを変更し適用をクリックした後、変更を有効にするために再起動しなければならないことのアラートが表示されます。再起動には約 10 ～ 15 秒かかります。再起動後、もう一度ログインする必要があります。

ワイヤレス > ステータスページ

この表示専用ページは、以下を行うために使用することができます。

- ワイヤレス インターフェースの状態を表示する
- ワイヤレス ネットワークの問題について、トラブルシューティングを行う

Wireless （ワイヤレス）> ステータスページのフィールド

規制管轄	日本。
ESSID	ワイヤレス > ネットワークページで設定された ESSID を表示します。詳しくは「SBG900J でワイヤレス ネットワーク名を設定する」を参照してください。*WLAN の使用を許可されていない人物へ、ESSID を教えないでください。*
チャンネル	アクセス ポイントのラジオ チャンネルを表示します。混信が発生した場合、ワイヤレス > ネットワークページで異なるチャンネルを設定することができます。
RTS 閾値	ワイヤレス > ネットワークページで設定した、Request to Send Threshold（閾値の送信要求）を表示します。
フラグメント閾値	ワイヤレス > ネットワークページで設定した、フラグメント閾値を表示します。
MAC アドレス	SBG900J の MAC アドレスを表示します。
セキュリティ モード	ワイヤレス暗号化の種類を表示します。詳しくは「SBG900J で WPA を設定する」または「SBG900J で WEP を設定する」を参照してください。
MAC アクセス制御	MAC アドレス制御設定を表示します（「SBG900J の MAC アクセス制御リストを設定する」を参照してください）： • リストに記載されているステーションのみ許可する— MAC アクセス制御リストに記載されているクライアントのみ、WLAN にアクセスすることができます。
MAC アクセス制御リスト	アクセス権のあるワイヤレス クライアントの MAC アドレスを表示します（「SBG900J の MAC アクセス制御リストを設定する」を参照してください）。

ワイヤレス > ネットワークページ

以下を行うために、このページを使用します。

- SBG900J でワイヤレス ネットワーク名を設定する
- 他の WLAN 設定を行う

ワイヤレス > ネットワークページのフィールド

フィールド	説明
ワイヤレス	
ワイヤレス インターフェース有効化	ワイヤレス インターフェースを有効にする際、このボックスを選択します。
ESSID	近辺にある複数の WLAN と区別するため、SBG900J WLAN の固有ネットワーク名を設定します。*ワイヤレス > セキュリティー詳細ページで ESSID ブロードキャスト無効化を選択した場合、WLAN 上のすべてのクライアントは* SBG900J と同じ ESSID（ネットワーク名）を保持しなければなりません。最大 32 文字の、大小文字を区別した英数字が使用できます。デフォルト値は「Motorola」です。*デフォルト ESSID は使用しないことを強く推奨します。WLAN の使用を許可されていない人物へ、ESSID を教えないでください。*
チャンネル	ワイヤレス ラジオ チャンネルを設定します。デフォルトのチャンネルで混信が発生した場合、チャンネルを変更することができます。ワイヤレス操作用の最初のチャンネルが 1 でない国を除き、デフォルトは 1 です。

ワイヤレス > ネットワークページのフィールド (続き)

フィールド	説明
操作モード	SBG900J とワイヤレス クライアントとの通信方法を設定します。 • 11b/11g Standard（11b/11g 標準）— すべての IEEE 802.11b および IEEE 802.11g のクライアントが SBG900J と作動できるようにします。*ほとんどの場合で最も順応性のあるデフォルト設定の使用を推奨します。* • 11g Enhanced（11g 拡張）— ネットワーク上のすべての IEEE 802.11g クライアント アダプタが、IEEE 11g 拡張モードのパフォーマンス拡張機能をサポートしている場合のみ、このオプションを選択します。これはすべての IEEE 802.11g アダプタでサポートされているわけではありません。 • 11b のみ -14 チャネルまで使用可能です。
詳細設定	
送信電力	SBG900J ワイヤレス送信電力を 3、6、12、25、50、75、または 100%に設定します。デフォルトでは 100%になっています。以下の理由で、送信電力を低く設定することができます。 • 道路などの外への「漏電」を減らすため • コンピュータまたはノート型コンピュータを SBG900J の近くへ置いた場合にパフォーマンスを向上させるため 送信電力制御は IEEE 802.11 のオプション機能です。
RTS 閾値	Request To Send Threshold （閾値の送信要求）は、パケット送信前に SBG900J が RTS を発行する最小パケットサイズを設定します。多くのクライアントが SBG900J と関連付けられている場合や、クライアントが遠すぎて SBG900J は検出できてもお互いが検出できない場合、RTS 閾値を低く設定することによって問題が多少解消されます。0 ～ 2347 バイトを設定します。デフォルト値は 2347 です。
フラグメント閾値	パケットが断片化されるサイズを設定します（一つのパケットではなく、複数のパケットを送信）。通信の質が悪い場合または大きな混信がある場合、断片化閾値を低く設定することによって問題が多少解消されます。256 ～ 2346 バイトを設定します。デフォルト値は 2346 です。
ビーコン間隔	ワイヤレスネットワーク同期のために SBG900J によって送信されるビーコン フレーム間の時間を設定します。1 ～ 999ms で設定します。デフォルト値は 100ms です。
DTIM 間隔	DTIM (delivery traffic indication message) 間隔は、消費電力節約モードで操作しているワイヤレス クライアントが、SBG900J からのバッファされたブロードキャストまたはマルチキャスト メッセージを「受信待機」する前に経過したビーコン間隔数です。デフォルト値は 1 ビーコンです。

ワイヤレス > セキュリティ— 詳細ページ

SBG900J のワイヤレス送信の暗号化方法を設定するには、このページを使用します。このページの使用に関して詳しくは、「ワイヤレス LAN 送信の暗号化」を参照してください。SBG900J 上で WEP または WPA を有効に

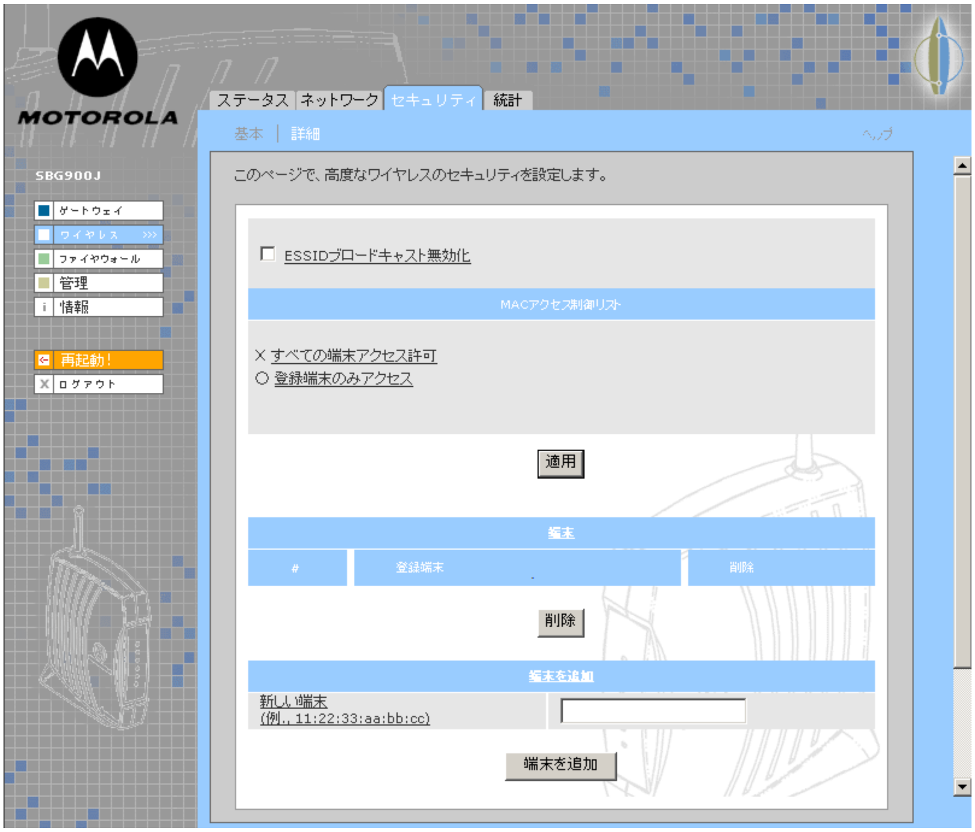
した後、「ワイヤレス クライアントを設定する」で記載されている通りワイヤレス LAN クライアントを設定しなければなりません。

注意！

> *デフォルトの設定のままでは、送信データのセキュリティが提供されていません。*

ワイヤレス > セキュリティ — 詳細ページ

このページを使用して、ワイヤレスセキュリティの詳細設定を行います。



ワイヤレス > セキュリティ — 詳細ページのフィールド

フィールドまたはボタン	説明
ESSID ブロードキャスト無効化	選択されている場合、SBG900J と同じネットワーク名 (ESSID) を持つワイヤレスクライアントのみ、SBG900J と通信することができます。閉鎖ネットワーク操作は IEEE 802.11b への SBG900J 拡張機能です。デフォルトでは選択されていません（オフ）。
MAC アクセス制御リスト	クライアント MAC アドレスに基づき、1 ～ 32 台のワイヤレスクライアントへワイヤレスへのアクセスを制限することができます。
リストに記載されているステーションのみアクセスを許可する	選択されている場合、MAC アクセス制御リストに記載されているクライアントのみ、SBG900J WLAN にアクセスすることができます。
適用	変更を適用する場合にクリックします。
リストに記載されている端末	登録ステーションのみアクセスが選択されている場合、MAC アクセス制御リストに記載されている、アクセス権を持つワイヤレスクライアントのリストを表示します。
削除	ワイヤレス クライアントを MAC アクセス制御リストから削除するには、そのクライアントの**削除**チェックボックスを選択し、**削除**ボタンをクリックします。
新しい端末の追加	
新しい端末	ワイヤレス クライアントの MAC アドレスを入力し、MAC アクセス制御リストへ追加します。形式として、*xx:xx:xx:xx:xx:xx* を使用します。MAC アクセス制御リストは 1 ～ 32 のクライアントを保持することができます。
端末を追加	クリックし、MAC アクセス制御リストへ新しい端末を追加します。

ワイヤレス > 統計ページ

このページを使用して、ワイヤレスの統計を表示することができます。

ワイヤレス > 統計ページのフィールド

フィールドまたはボタン	説明
送信されたフラグメント数	アドレス 1 フィールドのアドレスを伴う認識 MAC プロトコル データ ユニット (MPDU) 数あるいはタイプデータまたは管理のアドレス 1 フィールドのマルチキャストアドレスを伴う MPDU 数。
マルチキャスト送信フラグメント数	マルチキャスト ビットが、正常に送信された MAC サービス データ ユニット (MSDU) の受信先 MAC アドレスへ設定される時の送信断片数。ESS で STA として動作する際、これらのフレームが AP へ誘導される場合、これはすべての関連付けられた MPDU への確認が受信されたことを意味します。
失敗回数	送信試行回数が IEEE 802.11b の最短または最長試行上下限値を超過したため、MSDU が正常に送信されなかった回数。
リトライ数	1 またはそれ以上の再送信後に正常に送信された MSDU 数。

ワイヤレス > 統計ページのフィールド (続き)

フィールドまたはボタン	説明
複数リトライ数	1 回以上の再送信後に正常に送信された MSDU 数。
フレーム重複回数	シーケンス制御フィールドが、フレームが重複であることを示す受信フレーム数。
送信要求正常回数	RTS メッセージに応じて受信された CTS メッセージ数。
送信要求失敗回数	RTS メッセージに応じて受信されなかった CTS メッセージ数。
失敗回数通知	予期しながら受信されなかった、データ メッセージ送信からの通知メッセージ数。
受信フラグメント数	タイプ データまたは管理が正常に受信された MPDU 数。
マルチキャスト受信フラグメント数	マルチキャスト ビットが受信元 MAC アドレスに設定された時の MSDU 受信数。
フレームチェックシーケンスエラー数	受信した MPDU で検出された FCS エラー数。
送信フレーム数	正常に送信された MSDU 数。
WEP 復号不可能数	1 に設定された Frame Control（フレーム制御）フィールドの WEP サブフィールドおよびクライアント MAC アドレスへマップされた WEP キーの WEP サブフィールドを伴って受信されたフレーム数。これはフレームが暗号化されるべきでなかったか、受信クライアント側の WEP が有効になっていなかったため破棄されたことを示します。
更新	クリックすると新しいデータを収集します。

トラブルシューティング

ここに記載されている解決法によって問題が解決しない場合は、ご加入のケーブル プロバイダーへお問い合わせください。ケーブル プロバイダーへ問い合わせる前に、リアパネルにある Reset ボタンを押してみてください。SBG900J のリセットには 5 分から 30 分かかります。サービス プロバイダーは、「フロントパネルライトおよびエラー状態」に記載されているライトの状態を質問する場合があります。

問題	考えられる解決方法
POWER ライトが消えている	電源コードがコンセントおよび SBG900J へ適切に差し込まれているかどうかを確認してください。 コンセントが正常に動作しているかどうかを確認してください。 Reset ボタンを押してください。
データの送受信ができない	フロントパネルの上部で、どのライトが最初（左から）に消えているかに注目してください。「フロントパネルライトおよびエラー状態」で記載されている通り、このライトはエラーがどこで発生したかを示します。 ケーブルテレビを使用している場合、TV が写るかどうか、また、テレビ画像が乱れていないかを確認して下さい。通常のテレビチャネルを受信できない場合、データサービスが機能していません。 SBG900J の同軸ケーブルおよびコンセントを確認してください。必要があればきつく閉め直してください。 IP アドレスを確認してください。お使いのシステムの IP アドレスを確認するためのステップに従ってください。 イーサネットケーブルが SBG900J およびコンピュータへ適切に接続されていることを確認してください。
ワイヤレス クライアントでデータの送受信ができない	「データの送受信ができない」に記載されている最初の 4 つの点検を行います。 ワイヤレス > セキュリティー 詳細ページの**セキュリティ モード**設定を確認してください。 • SBG900J 上で **WPA** を有効にし、パスフレーズを設定した場合、影響を受ける各ワイヤレス クライアントが同じパスフレーズを持っていることを確認します。これにより問題が解決しない場合は、ワイヤレス クライアントが WPA をサポートしているかどうかを確認します。 • SBG900J 上で **WEP** を有効にし、キーを設定した場合、影響を受ける各ワイヤレス クライアントが同じ WEP を持っていることを確認します。これにより問題が解決しない場合は、クライアント ワイヤレス アダプタが SBG900J で設定した WEP キーの種類をサポートしているかどうかを確認します。 • 問題の原因を見つけるためセキュリティモードを一時的に停止するには、なしを選択してから適用をクリックします。*問題が解決したら、ワイヤレス セキュリティを必ず再度有効にしてください。* ワイヤレス > セキュリティー 詳細ページで : • **ESSID ブロードキャスト無効化**がオンになっていることを確認します。オンになっていない場合、影響を受ける各クライアント上のネットワーク名 (ESSID) が SBG900J 上の ESSID と同一であることを確認します。 • **リストに記載されている端末のみアクセスを許可する**を有効にしたかどうかを確認します。有効化されている場合、影響を受ける各ワイヤレス クライアントの MAC アドレスが正しくリストに記載されていることを確認します。 詳しくは「ワイヤレス LAN を設定する」を参照してください。
WPA が有効になっていると、無線伝送速度が遅い	ワイヤレス > セキュリティ―基本ページで、**WPA Encryption** type（WPA 暗号化の種類）が TKIP に設定されていることを確認します。すべてのワイヤレス クライアントが AES をサポートしている場合、「SBG900J で WPA を設定する」で記載されているステップ 4 に従い WPA Encryption（WPA 暗号化）を AES に変更してください。

フロントパネルライトおよびエラー状態

ライト	スタートアップ中に消灯する原因	通常動作中に消灯する原因
RECEIVE	ダウンストリーム受信チャンネルが取得できない	ダウンストリーム チャンネルを喪失した
SEND	アップストリーム送信チャンネルが取得できない	アップストリーム チャンネルを喪失した
ONLINE	IP 登録に失敗した	IP 登録が喪失した
POWER	SBG900J が電源コンセントへ適切に差し込まれていない	SBG900J の電源コードが抜けている

お問合せ先

SBG900 をレンタルおよびリースしている場合は、ケーブルテレビ会社へお問合せください。

カスタマーサービス、テクニカルサポートおよび保証請求についての情報は、SURFboard SBG900J に付属している*規制*、*安全性*、*ソフトウェアライセンスおよび保証情報*カードをお読みください。

一般的な質問への回答については、「よくある質問 (FAQ)」を参照してください。

よくある質問 (FAQ)

以下はお客様から寄せられるご質問への回答です。

Q 高速ケーブル インターネット アクセスとは何ですか？

A ケーブルインターネットアクセスは、電話回線の代わりにケーブルテレビのワイヤを使用してインターネットへ接続します。電話回線を使用しないため、電話での通話やファックスの着信の邪魔をしません。

Q **IEEE 802.11g** および **IEEE 802.11b** とは何ですか？

A IEEE ワイヤレスネットワークの標準規格です。

Q **SBG900J** にはどのようなワイヤレス セキュリティ対策が施されていますか？

A ワイヤレス接続上で送信されるデータを保護するため、SBG900J は WPA または WEP 暗号化および MAC アドレス制御リストをサポートしています。詳しくは「ワイヤレス セキュリティ」および「ワイヤレス LAN を設定する」をご覧ください。

Q **SBG900J** を使いながら、ケーブルテレビを見ることができますか？

A はい。インターネットの情報を送受信している間に、ケーブルテレビ回線はテレビシグナルを受信することができます。

Q **SBG900J** が作動しなくなった場合はどうすればいいですか？

A 「トラブルシューティング」に問題を診断するコツと、簡単な解決法が記載されています。問題が解決しない場合は、ケーブル プロバイダーへご連絡ください。

仕様

ワイヤレス

標準準拠	IEEE 802.11、IEEE 802.11b 直接シーケンス スペクトラム拡散 -DSSS、IEEE 802.11g
RF 周波数範囲	2.412 ～ 2.462 GHz（北米） 2.412 ～ 2.835 GHz（日本）
データ転送速度	1 Mbps DBPSK 2 Mbps DQPSK 5.5 または 11 Mbps CCK 6、9、12、18、24、36、48 または 54 Mbps OFDM
変調	1 Mbps DBPSK 2 Mbps DQPSK 5.5、11 Mbps CCK 6、9、12、18、24、36、48、54 Mbps OFDM
チャンネル数	日本 = 802.11b: 14, 802.11g: 13
送信電力	17.5 dBm (EIRP)
受信感度	11 Mbps で -83 dBm

ルータ

イーサネット標準準拠	IEEE 802.3、IEEE 802.3u
データ プロトコル	TCP/IP
ルーティング プロトコル	RIP V2
アップリンク ポート数	1

電気

入力電圧範囲	100 ～ 240 VAC、50 Hz ～ 60 Hz
消費電力	9 ワット

環境

動作温度	0 °C ～ 40 °C、-150 ～ 10000 ft.
保管温度	-30 °C ～ 80 °C
湿度	5% ～ 95% RH、結露のないこと
アンテナ	固定 (2)；内蔵 (1) および外部 (1)
LED インジケータ	Power、Receive、Send、Online、Internet、Wireless
インターフェース	AC 電源 (1)、F タイプ (1)、および RJ-45 (1)
ケーブル インターフェース	F コネクタ、雌、75Ω
CPE ネットワーク インターフェース	イーサネット 10/100Base-T（自動感知）
寸法	47.0（幅）x 149.1（奥行き）x 218.2（高さ）(mm)
重量	485 g （15.6 oz.— ユニットのみ）

ダウンストリーム

変調	64 QAM または 256 QAM
最大データ転送速度[a]	38 Mbps
帯域幅	6 MHz
最大シンボルレート	5.069 Msym/ 秒 (64 QAM) 5.361 Msym/ 秒 (256 QAM)
動作範囲	-15 ～ +15 dBmV
入力インピーダンス	公称 75 Ω
周波数範囲	88 ～ 860 MHz

アップストリーム (DOCSIS)

変調	QPSK または 8[b]、16、32[b]、64[b]、または 128[b] QAM
公称変調度	TDMA：160、320、640、1280、2560、および 5120 KHz S-CDMA：1280、2560、および 5120 KHz
最大データ転送速度[c]	30 Mbps
帯域幅	TDMA：200、400、800、1600、3200、および 6400 KHz S-CDMA：1600、3200、および 6400 KHz
周波数	5 MHz ～ 55 MHz（最小 / 最大）
シンボルレート	160、320、640、1280 および 2560 ksym/s
動作範囲（1 チャンネル）	TDMA： • +8 ～ +54 dBmV (32 QAM、64 QAM) • +8 ～ +55 dBmV (8 QAM、16 QAM) • +8 ～ +58 dBmV (QPSK) S-CDMA： • +8 ～ +53 dBmV（全変調）

a. 実際の速度は条件により異なります。アップロードおよびダウンロード速度はネットワークトラフィックおよびケーブル プロバイダーによって提供されるサービス、コンピュータ装置、サーバーの種類、サーバーへの接続数およびインターネット ルータの可用性を含みますがこれに限定されない要因の影響を受けます。

b. A-TDMA または S-DMA をサポートしている CMTS *のみ*。

c. 実際の速度は条件により異なります。最高速度 30Mbps は A-TDMA または S-CDMA 技術によって*のみ* 到達できます。

用語集

この用語集では、SBG900J で使用されている用語の定義および頭字語が記載されています。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

A

ALG

Application level gateway（アプリケーション レベル ゲートウェイ）トリガは、1 つまたはそれ以上のポートを開き、アプリケーションが正常に作動するようにするために、一部のファイル転送（例えば FTP）、ゲーム、ビデオ会議アプリケーションによって必要とされます。

AWG（アメリカン ワイヤ ゲージ）

電気コンダクタのサイズを指定するための規格システム。ゲージ数はサイズと反比例します。

ANSI

American National Standards Institute（米国規格協会）は、米国での標準開発のため取引企業、工業、専門協会によってサポートされる非営利の独立団体です。この団体は ASCII を定義し、国際標準化機構 (ISO) では米国を代表しています。

ANX

Automotive Network Exchange（自動車業界標準ネットワーク）

ARP

Address Resolution Protocol（アドレス解決プロトコル）は ホスト IP アドレスと一致する MAC アドレスを含む応答を得るため、データグラムのブロードキャストを行います。最初にネットワークに接続された時、クライアントは ARP メッセージを送信します。SBG900J は、その MAC アドレスを含むメッセージで応答します。その後、コンピュータによって送信されるデータは SBG900J MAC アドレスを受信先として使用します。

ASCII

The American Standard Code for Information Interchange（情報交換用米国標準コード）は、様々なデバイス間における処理および通信互換性のための英数字データを意味します。通常、非同期伝送に使用されます。

AUTO-MDIX

Automatic Medium-Dependent Interface crossover（自動クロスオーバー判別インターフェース）は、ポートの送信および受信ピンを自動的に反転させることにより、ケーブルエラーを探知・修正します。SBG900J イーサネット ポートおよび任意のコンピュータ、プリンタまたはハブ間で、ストレート ワイヤを使用できるようにします。

B

BCP

Binary Communication Protocol（バイナリ通信プロトコル）

BER

Bit Error Rate（ビット エラー レート）はエラービット数または一定の伝送ビット数から受信した文字数の比率です。

BPKM

Baseline Protocol Key Management（ベースライン プライバシーキー管理）は、ケーブルモデムまたはゲートウェイおよび CMTS 間のデータの流れを暗号化します。ケーブルモデムまたはゲートウェイが RF ネットワーク上のデータ プライバシーを確認するために登録を行った後で、暗号化されます。

bps

ビット / 秒

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

C

CableHome 家庭用ネットワーク デバイスへの高品質ケーブル系サービスの拡張のため、インターフェース 仕様を開発する CableLabs および技術提供者のプロジェクト。デバイスの相互運用性、QoS、およびネットワーク管理などの問題について取り上げています。CableHome により、ケーブル サービス プロバイダーは HFC で、より多くのサービスを提供することができます。家庭内全体にケーブルによるサービスを提供し、お客様の便宜性を向上します。

CableLabs ケーブルモデムのインターフェースの必要条件を定義し、テストを受けた装置が DOCSIS に準拠することを認定する研究機関

CMTS Cable Modem Termination System（ケーブル モデム終端システム）とは、IP ホスト、ケーブルモデムまたはゲートウェイおよび加入者を接続する HFC ネットワークのローカルまたは遠隔 IP ネットワークのインターフェースとなるケーブル システムのヘッドエンドでのデバイスのことです。すべてのケーブルモデムの帯域幅を管理します。エッジ ルータと呼ばれることもあります。

CNR Carrier to Noise Ratio（搬送波と雑音の比）

CoS Class of service（サービス クラス）トラフィック管理またはスケジュール機能は、データをアップストリームまたはダウンストリームで転送する際に行われます。

CPE Customer Premise Equipment（宅内装置）。通常コンピュータ、プリンタなどは、加入者の宅内にあるケーブルモデムまたはゲートウェイに接続されます。CPE は加入者またはケーブル プロバイダーが準備します。クライアントとも呼ばれます。

CSMA/CD Carrier Sense Multiple Access with Collision Detection（搬送波感知多重アクセス / 衝突検出方式）

D

dB デシベル

dBc 変調されていない信号レベルに相対する、dB で表される信号レベル。

DBm 特定のインピーダンスで 1 ミリワットを参照する計測単位。0dBm = 1 ミリワット (75Ω)

dBmV 1mV が 75Ω に渡る場合、参照電力への 75 Ω システムでの信号電力比として dB で表される信号レベル。

DHCP Dynamic Host Configuration Protocol（動的ホスト構成管理プロトコル）サーバーが、IP ネットワーク上のクライアント ホストへ IP アドレスを動的に割り当てます。DHCP では、IP アドレスおよびサブネットマスクを各クライアントへ「リース」するため、固定 IP アドレスの手動設定の必要がありません。使用していない IP アドレスの自動再利用を行います。

SBG900J *は DHCP クライアントであると同時に、DHCP サーバーでもあります。*

- ケーブル システム ヘッドエンドでの DHCP サーバーは外部 IP アドレスを SBG900J および任意で SBG900J LAN 上のクライアントへ割り当てます。
- SBG900J には、内部 IP アドレスをクライアントへ割り当てるビルトイン DHCP サーバーが含まれます。

DMZ 「非武装地帯」は、プライベート LAN およびインターネット間で論理的に位置する 1 台またはそれ以上のホストです。DMZ は、外部ユーザーによるプライベートデータへの直接アクセスを防ぎます。（この用語は北朝鮮と韓国などの対立国に位置する休戦ラインに由来しています。）小さな DMZ の典型的な設定では、DMZ ホストはプライベート LAN ユーザーから外部ウェブサイトへのアクセス要求を受け取り、これらの要求のためセッションを初期化します。DMZ ホストはプライベート LAN へ戻りセッションを初期化することができません。プライベート LAN 外部のインターネット ユーザーは DMZ ホストへのみアクセスすることができます。内部データを開示することなく、ウェブ サーバーやゲームの設定に DMZ を使用することができます。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

DNS	Domain Name System（ドメイン名システム）はドメイン名を IP アドレスへ変換するインターネットのシステムです。DNS サーバーは、Internetname.com などのドメイン名と 192.169.9.1 などの IP アドレスが一致する表を含んでいます。ワールド ワイド ウェブへアクセスする際、DNS サーバーはブラウザに表示される URL をウェブサイトの宛先 IP アドレスへ変換します。DNS ルックアップ表は配布されたインターネット データベースです。すべてのドメイン名とそれに一致する IP アドレスを含むリストを持つ DNS サーバーはありません。
DOCSIS	Cable Labs Data-Over-Cable Service Interface Specification（データ・オーバー・ケーブル・サービス・インターフェース仕様）の略で、HFC ネットワークおよびコンピュータシステムまたはテレビ間でデータを送信するケーブルモデム、ゲートウェイおよびサポート機器用のインターフェース標準を定義しています。ケーブルモデム標準として使用されていることを強調し、DOCSIS は CableLabs 認証ケーブルモデムと呼ばれています。Euro-DOCSIS は欧州で使用するために改訂された DOCSIS です。
DSSS	Direct Sequence Spread Spectrum（直接拡散方式）
Dotted-decimal（点区切り 10 進数）形式	オクテットと呼ばれる 4 つの 10 進数を使用し、IP アドレスまたはサブネットマスクを表現する方法。各オクテットは 8 ビットを表します。 クラス CIP アドレスのオクテットは「network.network.network.host」です。最初の 3 つのオクテットはネットワークアドレスを表し、最後のオクテットはホストのアドレスを表します。SBG900J LAN のデフォルト設定では、192.168.100 でネットワーク アドレスを表します。最後のオクテットにより、ホスト アドレスは 2 ～ 254 で表されます。
DSL	Digital Subscriber Line（デジタル電話加入者回線）
DSSS	Direct Sequence Spread Spectrum（直接拡散方式）は IEEE 802.11b RF 変調プロトコルです。

E

ESSID	拡張サービス セット ID またはネットワーク名は、同じエリア内の複数のワイヤレス LAN を区別するために、ワイヤレスクライアントがアクセス ポイントと関連付けるために使用する固有識別子です。ワイヤレス LAN 上のすべてのクライアントはアクセス ポイントと同じ ESSID を保持していなければなりません。SBG900J では、ESSID を Wireless（ワイヤレス）>NETWORK（ネットワーク）ページで設定することができます。
Euro-DOCSIS	欧州で使用するために改訂された DOCSIS である tComLabs 標準。
EAP	Extensible Authentication Protocol（拡張可能認証プロトコル）

F

FCS	Frame Check Sequence（フレーム チェック部）
F タイプ 3 コネクタ	SBG900J などの装置へ同軸ケーブルを接続するために使用されるコネクタ。
FEC	Forward Error Correction（フォワード エラー コレクション）は、送信元にデータの再送信を要求する必要なく伝送エラーを訂正する技術です。
FDMA	Frequency Division Multiple Access（周波数分割多重接続）は複数のユーザーが特定のラジオ スペクトラムを共有できるようにする方法です。各アクティブ ユーザーには、近辺のチャンネルから、チャンネル間隔と同量だけ各チャンネル オフセットの信号周波数と共に個別の RF チャネル（または信号）が割り当てられ、これにより各チャンネルの帯域幅を要求することができます。
FTP	File Transfer Protocol（ファイル転送プロトコル）はコンピュータ間でファイルを交換するためのインターネットの標準プロトコルです。FTP は、プログラムおよび他のファイルをインターネット上のウェブページからコンピュータへダウンロードする時に一般的に使用されています。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

G

GHz	ギガヘルツ—10 億サイクル / 秒。
GUI	Graphical User Interface（グラフィカル ユーザー インターフェース）

H

H.323	インタラクティブ ビデオ会議、データ共有および VoIP などのオーディオ アプリケーション用に ITU によって作成された一組のプロトコル。
HFC	ファイバーおよび同軸ケーブルのハイブリッド ネットワークであり、光ファイバー ケーブルをトランクとして使用し、同軸ケーブルを加入者の宅内で使用します。
hop	IP ネットワーク上の 2 つのルータ間の距離。パケットが受信先に向かって移動する hop 数はパケットのヘッダに保存されます。例えばホップ数が 6 である場合、パケットは 6 台のルータを通過したことを意味します。パケット hop カウントは TTL（有効期限）が減少するにつれ、増加します。
HTML	Hyper Text Markup Language（ハイパー テキスト マークアップ言語）
Hz	ヘルツ—1 サイクル / 秒。最高から最低状態の電磁気信号サイクルを変更する周波数を計測する単位。音声およびデータ通信でしようされる電磁気スペクトラムの帯域を定義するため、あるいは伝送媒体の帯域幅を定義するために使用されます。

I

IANA	IANA(Internet Numbering Address Authority（[インターネットの数字割り当て機関]）は、IP アドレス割り当てを監督するインターネット協会の IAB（Internet Architecture Board[インターネット アーキテクチャ審議会]）の下に存在する組織です。米国政府からの契約に基づいています。
ICMP	Internet Control Message Protocol（インターネット制御メッセージプロトコル）は、IP ホストおよびゲートウェイの間で送信されるエラー、問題、情報メッセージに使用されるプロトコルです。ICMP メッセージは IP ソフトウェアによって処理され、通常エンド ユーザーが見ることはありません。
ICSA	International Computer Security Association（国際コンピュータセキュリティ協会）は、調査、情報および製品認定に関するセキュリティ業界の主要情報源です。
IEEE	Institute of Electrical and Electronics Engineers（米国電気電子技術者協会）社 (http://www.ieee.org) は標準、技術書、電気および電子業界のシンポジウムを扱う組織であり、ANSI によって認可されています。
IEEE 802.11b **IEEE 802.11g**	IEEE ワイヤレス ネットワークの標準。
IEEE 802.3	*イーサネット*を参照してください。
IETF	Internet Engineering Task Force（インターネット技術標準化団体）(http://www.ietf.org) は、インターネット アーキテクチャを開発・維持するためのネットワーク設計者、操作者、販売者および調査者の公開国際社会です。技術作業グループが発行する作業文書を Internet-Draft（インターネット草稿）と呼びます。IETF は RFC(Requests for Comments) と呼ばれる草稿文書の再審議バージョンを発刊します。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◆ ボタンをクリックします。

IGMP	Internet Group Membership Protocol（インターネット グループ メンバーシップ プロトコル）はインターネット マルチキャスティングの標準です。IGMP は、マルチキャストルータがマルチキャスト パケットを転送するグループ マルチキャスト アドレスおよびインターフェースのデータベースを確立・維持します。 IGMP はマルチキャスト ホストおよびそれらの直接近辺マルチキャスト ルータを実行します。
IGMP スプーフィング	ルータがマルチキャスト ルータへマルチキャスト ホストおよび IGMP ホストに IGMP 要求者として行動する際の処理。
IP	Internet Protocol（インターネット プロトコル）は、インターネット上で異なる種類のコンピュータがお互いに通信し、データを交換することができるようにするための標準です。IP は一つの、途切れのない通信システムを提供し、インターネットを仮想ネットワークにします。
IP アドレス	TCP/IP ネットワーク上の各ホストを識別する固有の 32 ビット値。TCP/IP プロトコル ネットワークは、受信先 IP アドレスによってメッセージを転送します。IP アドレスには 2 つの部分があります。 • IANA によって割り当てられたネットワーク アドレス。 • SBG900J ネットワーク管理者は、自動的に DHCP サーバーを使用するか、または固定 IP アドレスとして、SBG900J に接続された各ホストへホストアドレスを割り当てます。 クラス C ネットワークでは、最初の 24 ビットはネットワークアドレスを表し、最後の 8 ビットはホストアドレスを表します。Dotted-Decimal（点区切り 10 進数）形式では、「network.network.network.host」のように表示されます。 SBG900J DHCP クライアントを WAN ページで有効にした場合、ケーブル プロバイダーは自動的にネットワーク アドレス、サブマスク、ドメイン名および DNS サーバーを割り当て、継続したインターネット接続を提供します。
IPSec	Internet Protocol Security protocol（インターネット プロトコル セキュリティ プロトコル）は、インターネット上での安全なパケット交換のための IETF 認証および暗号化標準です。IPSec は OSI 第 3 層で作動し、ネットワーク上のすべてを安全にします。
IKE	Internet Key Exchange（インターネットキー交換）
ISAKMP	Internet Security Association and Key Management Protocol（インターネット セキュリティ協会およびキー管理プロトコル）
ISDN	Integrated Services Digital Network（統合サービス デジタル網）
ISO	International Organization for Standardization（国際標準化機構）(http://www.iso.ch) は、世界約 140 国からなる連邦国際標準団体です。ISO は、物品およびサービスの国際取引の促進、知識、科学、技術および経済活動範囲での企業の発展により世界での標準化開発および関連活動を促進するため、1947 年に設立された非政府組織です。
ISP	Internet Service provider（インターネット サービス プロバイダー）
ITU	International Telecommunications Union（国際電気通信連合）

K

kHz	キロヘルツ—1000 サイクル / 秒。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◀ ボタンをクリックします。

L

L2F Layer 2 Forwarding（レイヤ 2 転送）は、ユーザーおよび企業ネットワーク間の仮想 PPP 接続を作るため、インターネット上での安全なトンネルを確立する OSI 第 2 層プロトコルです。L2F は最も確立され、安定したレイヤ 2 トンネリング プロトコルです。

L2TP レイヤ 2 トンネル プロトコルは、ISP が VPN を運営できるようにする PPP の延長です。L2TP は PPTP および L2F の最も優れた特徴を合わせたものです。L2TP は新しい IETF 標準です。

LAC L2TP Access Concentrator（L2TP アクセス コンセントレータ）は PPP フレームが LNS へトンネルされるクライアントが直接接続する装置です。LAC は L2TP が 1 つ以上の LNS へのトラフィックを伝送するための操作する媒体のみを実装する必要があります。LAC は、PPP 内で伝送されるどのプロトコルもトンネルする可能性があります。LAC は着信通話を初期化し、発進通話を受け取ります。LAC は L2F NAS と類似しています。

LAN Local Area Network（ローカル エリア ネットワーク）は建物または構内など、限られたエリア内で常時、高速帯域幅接続を提供します。イーサネットは最も広く使用されている LAN の標準です。

LCP Link Control Protocol（リンク制御プロトコル）は、PPP によって使用されるデータリンク接続を確立、設定およびテストします。

LED Light-Emitting Diode（発光ダイオード）

LNS L2TP Network Server（L2TP ネットワーク サーバー）は、PPP フレームが処理され、高いレベルのレイヤ プロトコルへ渡される L2TP トンネルの端末点です。LNS は PPP を終了する任意のプラットフォームを操作することができます。LNS は L2TP プロトコルをサーバー側で扱います。L2TP は L2TP トンネルが到着する単一媒体にのみ依存します。LNS には単一 LAN または WAN インターフェースがありますが、PPP インターフェース（非同期、同期、ISDN、V.120 など）の LAC の全範囲に到着した通話を終了することができます。LAC は発進通話を初期化し、着信通話を受け取ります。LNS は L2F 技術の家庭内ゲートウェイと類似しています。

M

MAC アドレス Media Access Control（メディア アクセス制御）アドレスは、各イーサネットネットワーク デバイスを識別するために、工場で ROM に永久保存された 48 ビットの固有値です。連続した 12 の十六進数で表現され、SBG900J の底面ラベルに印刷されています。ケーブル プロバイダーへ HFC MAC アドレスを提示する必要があります。イーサネット アドレス、物理アドレス、ハードウェア アドレスまたは NIC アドレスとも呼ばれます。

MB 1 メガバイト。1,024 x 1,024 バイト、1,024 キロバイトまたは約 800 万ビットに等しい。

Mbps 100 万ビット / 秒（メガバイト / 秒）。データ転送速度。

MIB Management Information Base（管理情報ベース）は、デバイスの設定、監視、またはテストのため、SNMP マネージャやエージェントによって使用されるソフトウェア オブジェクトの階層的な構造です。

MHz メガヘルツ—100 万サイクル / 秒。ラジオ周波数の計測単位。

MPDU MAC protocol data unit（MAC プロトコル データ ユニット）

MSDU MAC service data unit（MAC サービス データ ユニット）

MSO Multiple Systems Operator（複数システム操作者）。一つ以上のケーブルシステムを所有および運営する企業のこと。グループ運営者とも呼ばれます。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◆ ボタンをクリックします。

MTU Maximum Transmission Unit（最大転送単位）は、一定の物理的ネットワークにおいて、伝送可能な一つの連続していないメッセージのデータ最大量です。MTU には、一つのフレームでネットワークによって転送することのできるメッセージ サイズの上限があります。MTU を超えたメッセージは、送信前に断片化され、受信先で再編成なければばなりません。

mW ミリワット

N

NAS Network Access Server（ネットワーク アクセス サーバー）

NAT Network Address Translation（ネットワーク アドレス変換）は、内部トラフィック用に一組の IP アドレスを使用し、外部トラフィック用に次の一組を使用するための LAN のインターネット標準です。NAT は、SBG900J LAN コンピュータの IP アドレスをインターネット上で不可視にすることにより、ある種のセキュリティを提供します。

NAT がゲートウェイページで有効に設定されている場合、各外部 IP アドレスとクライアント IP アドレスの 1 対 1 マッピングがあります。

NAPT Network Address Port Translation（ネットワーク アドレス ポート変換）は、外部および内部 IP アドレス間の最も一般的なアドレス変換形式です。NAPT は一つの外部 IP アドレスを多くの内部 IP アドレスへマッピングします。 NAPT がゲートウェイページで有効に設定されている場合、一つの外部 IP アドレスは最大 245 の LAN クライアントの個々の内部 IP アドレスへマッピングされます。

NEC National Electrical Code（米国電気規約）—州および地方自治体による義務的な適用にふさわしい電気配線や器具の製造および設置に関する規則。

NIC Network Interface Card（ネットワーク インターフェース カード）はコンピュータデータを、LAN 上で送信できるパケット形式のシリアル データに変換します。NIC は拡張スロットにインストールしますが、内蔵されている場合があります。各イーサネット NIC には MAC アドレスがあり、カードの ROM に永久保存されています。

O

OSI Open Systems Interconnection（オープン システム間相互接続）リファレンス モデルは、データが送信元ホストのアプリケーションから受信先ホストのアプリケーションへどのようにネットワークを通じて移動するかを説明する実例的モデルです。ISO によって開発された概念的なフレームワークであり、現在、相互コンピュータ通信の主要モデルとなっています。OSI はモデルのみです。特別なネットワーク インターフェースを定義していません。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面） ボタンをクリックします。

P

PacketCable 双方向 HFC ケーブル設備上で、進歩したリアルタイム マルチメディア サービスを提供するための共通プラットフォームを定義する、CableLabs が先行するプロジェクト DOCSIS 1.1 を基礎とした PacketCable ネットワークは、高容量マルチメディア アーキテクチャの基礎として IP 技術を使用します。

PAT Port Address Translation（ポート アドレス変換）

PCI

PCMCIA Personal Computer Memory Card International Association（パーソナル コンピュータ メモリ カード国際協会）は、周辺機器を携帯コンピュータへ接続するための国際標準を制定します。ノート型コンピュータには一般的に PCMCIA スロットがあり、イーサネット接続などの機能を提供する 1 つまたは 2 つの PC カードを使用することができます。

PDA Personal Desktop Assistant（パーソナル デスクトップ アシスタント）

PDU Protocol Data Unit（プロトコル データ単位）は SNMP で使用される操作指示を含むメッセージです。基本 SNMP V2 PDU タイプは get-request、get-next-request、get-bulk-request、response、set-request、inform-request および trap です。

PING 小さなパケットをホストに送信し、応答を待つことによって、ホストへの到達是非をテストするネットワーク ユーティリティ。コンピュータの IP アドレスを PING し、応答を受信した場合、ネットワークでそのコンピュータへ到達することができます。「Packet InterNet Groper」の頭字語です。

PMD オープンシステム間の特定の種類の伝送リンク上で、ビットまたはビット グループを送信する物理層の物理的媒体に依存した副次的層。それは電気的、機械的およびハンドシェーキング方式を要します。

POTS PSTN を通じて提供される「Plain old Telephone Service（従来型の電話サービス）」。基本アナログ電話サービス。POTS はツイスト ペア ワイヤで最低の 4 kHz 帯域幅を使用します。

PPP Point-to-Point Protocol（ポイント ツー ポイント プロトコル）は、一般的にシリアルライン上の単純なリンクで、他のプロトコルを輸送するために使用されます。ダイヤルアップモデムにアクセスするために最も一般的に使用されます。

PPTP Point-to-Point Tunneling Protocol（ポイント ツー ポイント トンネリング プロトコル）は他のプロトコルをカプセル化します。複数のベンダーが共同で開発した、VPN を作成する新しい技術です。

Protocol データ交換についての正式な規則および規約。異なる種類のコンピュータ（例えば PC、UNIX または大型汎用機）が共通のプロトコルをサポートしている場合、お互いに通信することができます。

PSTN Public Switched Telephone Network（公衆電話交換網）は従来の回路交換の音声型電話網のことです。*POTS* も参照してください。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◆ ボタンをクリックします。

Q

QAM — Quadrature Amplitude Modulation（直交振幅変調）はデータの複数ビットを一つの信号要素に符号化するため、振幅と位相変調を使用します。QAM は振幅または位相変調単体よりも高速にデータを転送することができますが、ノイズによるエラーが発生する確率が高くなります。QAM は、QPSK などの他の変調形式よりも高い CNR を伴う伝送回路を必要とします。QAM には二種類あります。

- 16QAM は最大 16 の振幅および位相の組み合わせの一つとして、4 ビット / 記号を符号化します。
- 64QAM は最大 64 の振幅および位相の組み合わせの一つとして、6 ビット / 記号を符号化します。

QPSK — Quadrature Phase Shift Key（四位相偏移）変調は、他の記号と位相が 90 度異なる記号を伴い、各記号につき 2 ビットの情報を送信します。座標 (0、0 ～ 0、1 ～ 1、0 ～ 1、1) によって表される 4 つの信号配置点は、4 つの組み合わせを表します。

QoS — Quality of service（品質保証機能）は接続の優先順位、遅延、スループットおよび帯域幅について説明しています。

R

RADIUS — リモート認証ダイアルインユーザーサービスサーバーは通常大企業の設定で使用されます。

RAS — Remote Access Server（リモート アクセス サーバー）

RF — Radio Frequency（無線周波数）—HFC でデータを送信するための、CMTS 送信機および受信機によって使用される信号。搬送波はケーブルネットワークでの伝送用にデジタル データ ストリームを符号化するため変調されます。

RFC — IETF または他のウェブサイトで公開される Request for Comments（コメント要求）。多くの RFC が国際標準となっています。

RJ-11 — 家庭内または事務所の電話に最もよく使われているタイプのコネクタ。

RJ-45 — 8 ピンのモジュラ コネクタ。10Base-T または 100Base-T イーサネット ネットワークで最もよく使われるタイプのコネクタ。

ROM — Read-Only Memory（読み出し専用メモリ）

RTS — Request to Send（送信要求）

S

SID — Service ID（サービス ID）は、送信トラフィック種類を識別する（例えばデータまたは音声）ケーブルモデムまたはゲートウェイへ CMTS によって割り当てられる固有の 14 ビット識別子です。SID は、ケーブルモデムへ帯域幅の配分を行い、Cos を実装するための CMTS の基礎を提供します。

SDU — Service Data Unit（サービス データ ユニット）

SME — Small and Medium Enterprise（中小企業）

SMTP — Simple Mail Transfer Protocol（簡易メール転送プロトコル）は E メールを転送するためのインターネットの標準プロトコルです。

SNMP — Simple Network Management Protocol（簡易ネットワーク管理プロトコル）はネットワークおよびネットワーク デバイスを監視および管理するための標準です。データは PDU メッセージを使用して交換されます。

SOHO — Small Office Home Office（小規模な事業者や個人事業者）

SYSLOG — 正式でない業界規格であるログ記録システムイベントの UNIX 標準。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◀ ボタンをクリックします。

T

TBCP　Tagged Binary Communication Protocol（タグ付きバイナリ通信プロトコル）

TCP　OSI の 4 層であるトランスポート層上の Transmission Control Protocol（伝送制御プロトコル）は、IP（ネットワーク層の 3 層）ネットワーク上でのデータ送信に信頼性の高い輸送を提供します。接続されていない IP に加え、ホスト間のデータ交換のための規則および手順を定義するエンドツーエンド プロトコルです。TCP は、要求があれば未解決パケットの追跡、着信パケットのエラーチェック、パケットの再送信のため、タイマーを使用します。

TCP/IP　Transmission Control Protocol/Internet Protocol（伝送制御プロトコル / インターネットプロトコル）は、インターネット上に存在するネットワーク間のデータ通信の標準および規則を提供します。世界中のインターネットワーキングの標準であり、インターネットの基本通信プロトコルです。

TFTP　Trivial File Transfer Protocol（簡易ファイル転送プロトコル）はファイルを転送するために使用される簡易プロトコルです。

TKIP　Temporal Key Integrity Protocol（一時キー完全性プロトコル）

TTL　有効期限は、パケットが破棄されるまえに通過することができるルータ数（または hop 数）です。ルータがパケットを処理する時、TTL を一つ減らします。TTL がゼロに到達したら、パケットは破棄されます。

U-W

UDP　User Datagram Protocol（ユーザー ダイアグラム プロトコル）

USB　Universal Serial Bus（ユニバーサル シリアル バス）はプリンタ、スキャナ、マウス、モデムまたはキーボードなどの追加機器用コンピュータ インターフェースです。USB は 12Mbps データ転送速度およびプラグ アンド プレイ インストールをサポートします。一つの USB ポートへ最大 127 台のデバイスを接続することができます。

UTP　Unshielded Twisted Pair（アンシールド ツイスト ペア）ワイヤ

VLAN　Virtual Local Area Network（仮想ローカル エリア ネットワーク）は同じ配線でつながれたかのように論理的に通信設定された、異なる LAN セグメントにあるデバイスのグループです。

VoIP　Voice over Internet Protocol（ボイス オーバー インターネット プロトコル）は音声、FAX および他の情報をインターネット上で交換する方法です。音声および Fax は、各線の専用回路を使用した PSTN の従来の電話線を使用していました。VoIP によって、共有線上へ連続していないデータパケットとして通話を送信することができるようになります。VoIP は、コンピュータ、電話およびテレビを一つの統合された情報ネットワークへ収束する最も重要な部分です。

VPN　Virtual Private Network（仮想プライベートネットワーク）は、安全で高速な接続を提供するため、公共ネットワーク（通常インターネット）から回送される「仮想」接続（トンネル）を使用した私設ネットワークです。通常、ユーザーは自宅または小規模のオフィスから遠隔操作します。VPN 接続は専用リンク（例えばリース線など）と同じようなセキュリティと性能を提供し、専用線より低価格です。

WAN　Wide Area Network（ワイド エリア ネットワーク）は国や世界全体など、広い地理での接続を提供します。帯域幅はニーズと予算によって異なりますが、通常 LAN よりもかなり安価となります。

WAP　Wireless Access Point（ワイヤレス アクセス ポイント）または Wireless Access Protocol（ワイヤレス アクセス プロトコル）。*アクセス ポイント*も参照してください。

WECA　Wireless Ethernet Compatibility Alliance（ワイヤレス イーサネット互換性連合）はすべてのワイヤレス デバイス（コンピュータ カード、ノート型コンピュータ、エア ルータ、PDA など）がお互いに通信できることを確実にするために作業を行う商業団体です。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◆ ボタンをクリックします。

WEP　Wired Equivalent Privacy encryption（ワイヤレス LAN 暗号化技術）はワイヤレス LAN で伝送されるデータのプライバシーを保護します。WEP は、伝送データの暗号化および解読にキーを使用します。アクセス ポイントは、データを他のクライアントへ転送する前にクライアントを認可しなければなりません。WEP は IEEE 802.11b の一部です。*WEP は使用が難しく暗号化が強力ではないため、可能であれば WPA を使用することを推奨します。*

WiFi　ワイヤレスの忠実度という意味で（読み方：ワイファイ）、IEEE 802.11b をサポートする製品に使用されるブランド名。

WLAN　ワイヤレス LAN

WPA　Wi-Fi Protected Access (WPA) 暗号化は、Wi-Fi Alliance Wi-Fi Protected Access （Wi-Fi 保護アクセス）ウェブページ (http://www.wifialliance.org/OpenSection/protected_access.asp) で記載されている通りです。WEP よりも強固な暗号化を提供します。*すべてのクライアントハードウェアが WPA をサポートしている場合、WPA を使用するよう推奨いたします。*

あ

アクセス ポイント　ワイヤレスクライアント（ステーション）にワイヤレス LAN の接続を提供するデバイス。
SBG900J はワイヤレス アクセス ポイントとしての役割をします。

アダプタ　コンピュータ、プリンタ、または他の周辺機器をネットワークまたは他のデバイスへ接続するデバイスまたはカード。*ワイヤレス アダプタ*はコンピュータをワイヤレス LAN へ接続します。

アップストリーム　ケーブルデータ ネットワークでは、アップストリームはインターネットから加入者のコンピュータへケーブルモデムを通して CMTS およびインターネットへ送信されたデータの方向を表します。

アドレス変換　*NAT* を参照してください。

暗号化　データを符号化すること。

い

イーサネット　最も幅広く使用されている LAN の種類。IEEE 802.3 としても知られています。最も一般的なイーサネット ネットワークは 10Base-T であり、伝送速度は最大 10 Mbps です。通常、RJ － 45 コネクタが端に付いたシールドされていない、ツイスト ペア ワイヤを使用します。高速イーサネット (100Base-T) は最大 100Mbps の転送速度を提供します。「Base」は「ベースバンド技術」を意味し、「T」は「ツイスト ペア ケーブル」を意味します。

各イーサネット ポートには、MAC アドレスと呼ばれる物理的アドレスがあります。

イベント　オペレータまたはネットワーク管理システムに何かが発生したことを知らせる、デバイスによって生成されたメッセージ。

インターネット　TCP/IP を使用した、世界的に相互接続されたネットワークの集合。

インターネットワーク　集合に存在する任意のネットワークに接続されたすべての機器と通信することができる相互接続されたネットワークの集合。

インピーダンス　デバイス内における、交流電子電流の流れに対する全体抵抗。同軸および他の CATV 部品におけるインピーダンスは典型的に 75 Ω です。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◀ ボタンをクリックします。

え

エンド ポイント VPN エンドポイントは VPN をルータで終了させ、SBG900J LAN 上のコンピュータが VPN クライアントソフトウェアによってインターネットを経由して VPN サーバーへトンネルする必要がないようにします。

お

オーム 電気抵抗の単位。

か

回路交換網 各接続にその存続期間中専用回線が必要となる通常の PSTN 電話ネットワークで使用されるネットワーク接続の仕組み。その他に、パケット交換網があります。

外部 IP アドレス ケーブル サービス プロバイダーによって SBG900J へ割り当てられた IP アドレス。外部 IP アドレスはインターネット上の他のデバイスから見ることができます。*内部 IP アドレス*も参照してください。

拡張スロット 新しい機能を追加するために基板を挿入することができる、コンピュータ内の接続ポイント。

カプセル化 含まれたデータ形式を隠すため、データを他のデータ ユニットに含むこと。

加入者 ケーブル プロバイダーからテレビ、データまたは他のサービスにアクセスする家庭またはオフィス ユーザー。

く

クライアント クライアント / サーバー アーキテクチャにおいて、クライアントとはファイル転送、遠隔ログインまたはサーバーからの印刷などのサービスあるいはファイルを要求するコンピュータのことです。CPE とも呼ばれます。

ワイヤレス LAN では、クライアントとはアクセス ポイントと通信できる任意のホストを意味します。ワイヤレスクライアントは「ステーション」とも呼ばれます。

クラス C ネットワーク 最大 253 台のホストを含む IP ネットワーク。クラス C の IP アドレスは「network.network.network.host」の形式を使用しています。

クロストーク 不必要な信号が必要な信号を妨害すること。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

け

経由し　SBG900J LAN 上のパススルー クライアントはケーブル プロバイダーの DHCP サーバーから外部 IP アドレスを取得します。

ゲイン　信号が上がる範囲。高ゲイン アンテナは、信号が伝達する距離を増やしながらも使用できるため、ワイヤレス信号レベルを上げます。

ゲートウェイ　異なるプロトコルを使用してネットワーク間で通信できるようにするデバイス。*ルータ*. も参照してください。

SBG900J によって、IEEE 802.11b、イーサネットをサポートする最大 253 台のコンピュータが一つのブロードバンド インターネット接続を共有することができるようにします。

ゲートウェイ IP アドレス　インターネット上のデフォルト ゲートウェイ ルータのアドレス。「giaddr」としても知られています。

ケーブルモデム　HFC ネットワーク上でデータ通信を提供するため、加入者が使用する場所にインストールされるデバイス。特記のない限り、本文書で使用される「ケーブルモデム」とは DOCSIS または Euro-DOCSIS ケーブルモデムのみを意味しています。

ケーブルモデム設定ファイル　登録時にケーブルモデムまたはゲートウェイがケーブル プロバイダーの TFTP サーバーからダウンロードする操作パラメータを含むファイル。

減衰　装置ロス、伝送ラインまたは他のデバイスによる、伝送および受信電力の差。通常、デシベルによって表されます。

こ

固定 IP アドレス　ホストへ永久的に割り当てられた IP アドレス。通常、固定 IP アドレスは手動で割り当てる必要があります。動的 IP アドレスの対義語。

さ

サーバー　クライアント / サーバー アーキテクチャにおいて、クライアントへファイル転送、遠隔ログインまたは印刷などのサービスあるいはファイルを提供する専用コンピュータ。

サービス プロバイダー　ケーブル データ サービスを加入者へ提供する会社。

雑音・ノイズ　電気エネルギーあるいはインターフェースの無作為な噴出。テレビ画像が砂の嵐状態になることがあります。

サブネット マスク　ネットワーク アドレスを決定するため、パケットの受信先 IP アドレスを論理的につながれたビットマスク。ルータはネットワーク アドレスを使用し、パケットをルート（回送）します。

サブネットワーク　ネットワークの一部。よく「サブネット」と省略されます。サブネットが使用される場合、IP アドレスのホスト部分はサブネットとホスト番号に分割されます。ホストおよびルータはサブネットマスクを使用し、ネットワークおよびサブネット番号で使用されるビットを識別します。

し

周波数　Hz、KHz、MHz または GHz で計測される、一定期間（通常 1 秒間）に電磁気信号が同一のサイクルを繰り返す回数。

十六進法　桁上りの前に基本ユニットとして 16 の連続した数字（0 ～ 9 および文字の A ～ F）を使用するシステム。コンピュータでは十六進数はバイナリ（二進数）を表現する時に便利な方法です。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

衝撃雑音 短期間のノイズ。一般的に約 10 マイクロ秒（100 万分の 1 秒）電圧スパイク、電動機の開始、落雷または交換機器など、ケーブルから流れ出る電気過渡現象によって発生します。

シンボル レート ボーレートとしても知られ、状態（周波数、電圧レベルまたは位相角度の状態）間で異なるまたは変化させる通信チャンネルにある信号の回数 / 秒を計測する単位。通常、シンボル / 秒 (sps) で計測されます。

す

スイッチ イーサネット ネットワークでは、ブリッジと類似した方法で MAC アドレスに基づくスイッチ フィルタフレーム。スイッチは、二つ以上のセグメントを接続することができるので、より高度です。

スコープ DHCP サーバーがクライアントに貸し出す（リースする）IP アドレス。

ステーション IEEE 802.11b の用語で、ワイヤレス クライアントのこと。

ステートフル インスペクション 正当性を確認するため、ファイヤーウォール インターフェースを追加する各接続を探知するファイヤーウォールの一種。固定規則に基づいたパケットヘッダに含まれる送信元および受信先の点検の他に、ファイヤーウォールは、

- ファイヤーウォールを探知した前のパケットによって確立されたコンテキスト上でパケットヘッダを点検します。
- 接続状態を監視し、テーブルにその状況を保存します。
- 特定のポートへの接続が要求されるまで、ポートを閉じます。
- 送信元および受信先以上の情報が含まれていないかどうかを決定するため、アプリケーション層までのパケットの内容を点検することがあります。

ステートフル インスペクション ファイやウォールは静的フィルタ ファイヤーウォールよりも高等です。

スペクトラム 電磁気信号の伝送に使用される特定の周波数範囲。

スペクトラム配分 AM、FM またはパーソナル通信など、特定のサービスのための利用可能な電磁気スペクトラム部分の配分。

せ

静的フィルタ 管理者が定義した規則にのみ基づき、パケット ヘッダ の 送信元および受信先を点検するファイヤーウォールの一種。

静的ルート 手動で定義されたルート。

全二重 データの送受信を同時に行うことができること。*半二重*も参照してください。

そ

双方向 ヘッドエンドから加入者へ、または加入者からヘッドエンドへの両方向で信号を伝送することができるケーブルシステム。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

た

帯域幅　周波数範囲における、媒体の伝送容量。帯域幅が大きいと、一定時間に伝送するデータ量も多いことを示します。

ダウンストリーム　ケーブル データ ネットワークでは、ダウンストリームはインターネットからコンピュータによって受信されたデータの方向を表します。

ダウンロード　ファイルを 1 つのコンピュータから他のコンピュータへコピーすること。ファイルをサーバーからコンピュータへダウンロードするために、インターネットを使用することができます。DOCSIS または Euro-DOCSIS ケーブルモデムまたはゲートウェイはスタートアップ中、TFTP サーバーから設定ファイルをダウンロードします。

て

定期的調整　最初の調整が行われた後で、継続的に行われる調整のこと。

ディストーション　伝送媒体内での信号波の必要のない変更。入力波形の非線形再生。

データグラム　RFC1594 では、データグラムは「自発的で独立した、送信元および受信先コンピュータとトランスポート ネットワーク間における早期交換に依存することなく、送信元から受信先コンピュータへ回送するのに十分な情報を伝送するデータの実体」と定義されています。ほとんどの場合、パケットという用語が代わりに使用されています。

デフォルト ルート　ルーティング表にある他のルートが使用できない場合、パケットが転送されるルート。

と

透過ブリッジ　有線イーサネット LAN、ワイヤレス LAN 上にあるすべてのホストが同じ物理的ネットワークに接続されているかのように通信できるようにする方法。

動的 IP アドレス　DHCP サーバーによってホストへ一時的に貸し出し（リース）される IP アドレス。*固定 IP アドレス*の対義語。

同軸ケーブル（コアックス）　中心ワイヤの周囲を絶縁体、編み込まれたワイヤのシールドによって囲まれたケーブルの種類。シールドは電気および無線周波妨害を最小限に抑えます。同軸ケーブルは、広帯域幅用に使用され、長距離伝送をサポートすることができます。

登録　ケーブルモデムを CMTS へ知らせる方法。ケーブルモデム設定ファイルおよび認証が確認され、CoS によって取り決められます。

ドメイン名　motorola.com など、IP アドレスをマップする固有名。ドメイン名は通常、IP アドレスより覚えるのが簡単です。

ドライバ　コンピュータがネットワークまたは他のデバイスと相互作動できるようにするソフトウェア。例えば、プリンタ、モニタ、グラフィックアダプタ、モデム、イーサネット、HPNA など、その他多くのドライバがあります。

トランスポート層　エラー認識および回復のためのプロトコルを考慮した OSI の層 この層は情報フローも統制します。

トランク　データが送信される電子的なパス。

トンネル　パケットを、ネットワーク上で送信するために他のパケットの中に入れること。同封パケットのプロトコルはパケットがネットワークに入出する各エンドポイントまたはトンネル インターフェースによって理解されます。VPN は安全なネットワークを作るため、トンネリングに依存しています。

トンネリングには以下の種類のプロトコルが必要となります。

- データが送信されるネットワークが使用する、TCP などの送信プロトコル
- IPSec、L2F、L2TP、または PPTP などの、元のデータを包むカプセル化プロトコル。
- IP など、元のデータのためのパッセンジャー プロトコル。

な

内部 IP アドレス　SBG900J の DHCP サーバーによって、一定のリース期間、SBG900J LAN 上にあるコンピュータへ割り当てられた IP アドレス。内部 IP アドレスは SBG900J LAN によってのみ使用されます。インターネット上のデバイスからは不可視です。*外部 IP アドレス*も参照してください。

に

認可　ベースライン プライバシーを有効にする CMTS とケーブルモデムまたはゲートウェイ間の処理の一部。

認証　CMTS が、パスワード、信頼 IP アドレスまたはシリアル番号を使用し、アクセスが認証されていることを確認する処理。

ね

ネットワーク　相互通信するために接続された 2 台以上のコンピュータ。ネットワークは通常、動種類のケーブル配線を使用して接続されています。

ネットワーク層　オープンシステムとの経路を確立するためのサービスを提供する OSI アーキテクチャの第 3 層。ネットワーク層は隣接ノードのアドレスを知り、ネットワークアドレスを伴う出力をパッケージ化し、経路を選択し、トランスポート層のローカル ホスト ドメインへの着信メッセージ認識し、転送します。

ネットワーク ドライバ　コンピュータが NIC と通信できるようにする NIC に付属するソフトウェア。

の

ノード　LAN では、すべてのネットワーク デバイスを表す総称的な用語。

HFC ネットワークでは、加入者の場所への光ファイバー トランクおよび同軸ケーブル提供者間のインターフェース。ノードは典型的に加入者の近辺にあります。

は

バイナリ　0 と 1 の 2 つの数字を使用した 2 進数。

パケット　インターネットまたは他のパケット交換ネットワークにおいて、送信者および受信先間を回送するデータ単位。E メール メッセージや他のファイルなどのデータがインターネット上で送信される時、送信者の IP はデータを固有番号の付いたパケットへと分割します。パケットのヘッダには受信先および送信元の IP アドレスが含まれています。各パケットは異なる通路を使用する場合があります。すべてのパケットが受信先へ到着した時、そこで IP はパケットを再構成します。ヘッダおよびデータの長さは様々です。パケットおよびデータグラムは類似した意味を持ちます。

パケット交換網　インターネットなどの、連結接続されていないネットワークの伝送を扱う構造。その他に、回路交換網があります。

ハブ　LAN では、ハブとは複数のホストと LAN を接続するデバイスのことです。ハブはデータのフィルタリングを行いません。*ブリッジ*および*ルータ*も参照してください。IP ハブは通常、ラックまたはデスクトップ上の機器です。

HFC ネットワークでは、ハブはシステムの一環として一部またはすべてのヘッドエンド機能を行う規模が縮小されたヘッドエンドです。

半二重　一台のデバイスのみがデータを送信することができるネットワーク。*全二重*も参照してください。

ひ

ピギーバッキング ケーブルモデムが同時にデータを送信し、帯域幅を追加要求する際に発生する処理。

ビット レート 一つの通信チャンネルで 1 秒間に伝送されるビット数（デジタル の 0 および 1）。通常、ビット / 秒あるいは bps で計測されます。

非同期タイミング SBG900J は、アップストリーム データ伝送に同期タイミングを使用します。帯域幅が利用できる CMTS ブロードキャスト メッセージです。SBG900J はミニ スロットを x 数必要とするデータ バイトを予約します。CMTS は特定の時間にデータを受信できると応答します（同期）。その特定時間に、SBG900J は x 数のデータバイトを送信します。

ふ

ファイヤーウォール インターネットおよび SBG900J LAN の間でアクセス制御ポリシーを強化する SBG900J 上のセキュリティ ソフトウェア システム。

復調 前に変調された波を元へ戻し、副搬送波で結合・変調された複数の信号を分解する操作。

符号化 電子信号を変え、権限のあるユーザーのみが情報を見ることができるように解読すること。

物理層 OSI アーキテクチャの第 1 層。オープン システム間の伝送リンク上でビットまたはビットのグループを送信するサービスを提供します。それは電気的、機械的およびハンドシェーキング方式を要します。

ブリッジ 類似したプロトコルを使用し、2 つの LAN を接続する、OSI 層の 2 のネットワーク デバイス。トラフィック量を減らすため、MAC アドレスに基づき、フレームをフィルタします。ブリッジは、他のグループとはあまり通信を行わないが、同じグループでは頻繁に通信を行う 2 つのグループのホスト間で置き換えることができます。ブリッジは、他の側へ伝送を行うかどうかを決定するために、各パケットの受信先を点検します。*スイッチ*も参照してください。

フレーム アドレスおよびプロトコル制御データを含むネットワーク ノード間を伝送されるデータ単位。制御フレームの中には、データを全く含まないものもあります。

フロー 一方向へ移動するデータ パス。

ブロードバンド 単一ケーブルで音声、ビデオ、データおよび他のインタラクティブ サービスを伝送する、複数の独立したキャリアを多重送信する広帯域幅ネットワーク技術 比較的大量のデータを一定時間に伝送することができる通信媒体。複数のチャンネルおよびサービスを伝送することができる技術について説明することができるケーブル TV の同義語としてよく使用されます。

ブロードキャスト 複数のネットワーク デバイスへの同時伝送。グループおよびユニバーサル アドレスをサポートするプロトコル構造。*マルチキャスト*および*ユニキャスト*も参照してください。

プロビジョン CMTS 上のケーブルモデムの自動発見または手動設定の処理。

分配器 2 つ以上のケーブル間の入力ケーブルからの信号を分配する機器。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◀ ボタンをクリックします。

へ

ベースライン プライバシー　CMTS およびケーブルモデムまたはゲートウェイ間のデータを暗号化するオプション機能。サービス保護は、MAC アドレスによって固有に識別されるケーブルモデムまたはゲートウェイが、アクセス権を与えられたサービス用にのみキーを取得することができるよう確実にすることによって提供されます。

ヘッダ　パケットの先頭にあるデータで、パケットに何が含まれているかを識別します。

ヘッドエンド　HFC ネットワーク上で変調する TV プログラム、ラジオプログラム、データおよび電話を受け取る場所。返りデータおよび電話による伝送も送信します。ヘッドエンド装置には送信機、前置増幅器、周波数端末、復調器、およびワイヤレスおよびケーブルチャンネルへの入力ブロードキャスト TV 信号を増幅、フィルタ、変換する他のデバイスが含まれます。

ほ

ポイント ツー ポイント　一つのポイントから他のポイントへの物理的な接続。

ボー　アナログ信号レート 複雑な変換モードでは、デジタル ビット レートは複数のビット / ボーに変換されます。例えば、64 QAM は 6 ビット / ボーに変換され、16 QAM は 4 ビット / ボーに変換されます。

ポート　コンピュータまたは他の電子的デバイスでは、ポートとは物理的にネットワークまたは他のデバイスとそれらを接続するソケットまたはプラグのことです。

TCP/IP では、ポートとはサーバープログラムを特定するためにクライアント プログラムによって論理的に使用される 0 ～ 65536 の数値のことを指します。ポートの 0 ～ 1024 は予約されています。

ポート トリガリング　特定のアプリケーションが着信通信を行えるようにする構造。主にゲームアプリケーションで使用されます。

ポート ミラーリング　SBG900J 上の一つのポート（コピー元）から調査される他のポート（コピー先）へコピーできるようにする機能。コピー先は、ネットワークを管理する人物が監視を行えるよう、コピー元ポート上の伝送された（元）または受信された（先）データをミラーします。

ホスト　IP において、ホストは完全双方向ネットワーク アクセスができるエンド- ユーザー アプリケーションまたはサービスをサポートする任意のコンピュータです。各ホストには、IP アドレスを作るネットワーク番号を合わせた固有ホスト番号があります。

ホストには、他に下記の意味があります。

- 団体または個人による 1 つ以上のウェブ サイト用にサーバーページウェブサーバーを実行しているコンピュータ。
- このサービスを提供する企業。
- IBM 環境での、大型汎用コンピュータ。

ま

マルチキャスト　一つの送信先から複数の受信先へ送信されるデータ伝送。*ブロードキャスト*および*ユニキャスト*も参照してください。

め

メディア（媒体）　信号が通過する多様な物理環境。例えば、同軸、アンシールド ツイスト ペアまたは光ファイバーケーブルなど。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）ボタンをクリックします。

ゆ

ユニキャスト　一つの送信先から一つの受信先へ送信されるポイント ツー ポイントのデータ伝送。これはウェブサイトにアクセスする一般的な方法です。*ブロードキャスト*および*マルチキャスト*も参照してください。

り

リターン ロス　ケーブルシステムとデバイスとの一致の質を計測する方法。リターン ロスはデバイスによって反映される電力量の比率です。好ましいリターンロスは 20dB 以上です。

流合雑音　ラジオ放送からケーブル施設が採取する連続していない周波数によって一般的に発生する雑音。あるいは適切に接地されていないか、シールドされていないヘア ドライヤーなどの家庭用電化製品によって発生する雑音。流合はケーブル システムの雑音の主要源です。

る

ルータ　IP ネットワークにおいて、少なくとも二つのネットワークを接続するデバイス。これらのネットワークは類似している場合も、類似していない場合もあります。ルータは一般的にネットワーク間の*ゲートウェイ*に設置されています。ルータは OSI ネットワーク第 3 層で操作されます。ルータは、IP アドレスを基に、送信元および受信先 IP アドレスを検証し、最適な転送経路を決定するため、パケット をフィルタします。

ルータは、ネットワーク スイッチ（交換機）の一部として含まれています。ルータはコンピュータのソフトウェアとして実装されていることもあります。

ルーティング表　パケットにとっても最適なルート（経路）を決定するための、ルータによって使用される利用可能なルートの一覧表。

ループバック　伝送信号を受信信号へループするテスト。通常、ループバック テストはネットワーク デバイスによって初期化されます。テストは通路を確認したり、通路上の信号量を計測したりするために使用されます。

れ

レイテンシ　信号がデバイスを通過するために必要とする時間。しばしば、記号量によって表現されます。

レイヤ（層）　ネットワークにおいて、レイヤ（層）とはソフトウェア プロトコル レベルのことです。各例はその上の層のための機能を行います。OSI は 7 つの機能層を持つ参照モデルです。

わ

ワイヤレス ケーブルモデムゲートウェイ　SBG900J ワイヤレス ケーブルモデムゲートウェイは、SOHO または SME での使用のため、ケーブルモデム、ルータ、イーサネットスイッチ、ワイヤレス アクセス ポイントおよび DHCP サーバーが一体化した単体デバイスです。

ワールド ワイド ウェブ　情報へナビゲートしたり、ハイパーリンクしたりするために使用するインターネットへのインターフェース。

前のページへ戻るには、Acrobat の Go to Previous View（前の画面）◆ ボタンをクリックします。

ソフトウェア ライセンス

Motorola Inc.、Broadband Communications Sector、所在地：101 Tournament Drive, Horsham, PA 19044

重要：いかなるソフトウェア、ファームウェアおよび関連文書（以下「ソフトウェア」）をダウンロード、インストール、ご使用される前に、本ソフトウェア契約書（以下「契約書」）とモトローラのケーブル・データ製品（以下「ケーブル・データ製品」）の添付文書を良くお読みください。ケーブル・データ製品を使用するためにいかなるソフトウェアをインストール、ダウンロード、そして使用した場合、お客様が本契約書の各条項に合意したものと見なします。本契約書はお客様とモトローラ社との合意の上で締結される法的な契約書です。本契約書条項は、本ソフトウェアを使用するお客様および本製品を受け継いで使用するいかなるユーザーを対象として適用されます。

本契約書の条項に同意されない場合、(I) 本ソフトウェアを未使用のまま、(II) すべてのコンポーネント、文書、その他ケーブル・データ製品に付属した全製品を含む、ケーブル・データ製品およびソフトウェア（すべてを含めて「製品」）を販売元またはご加入のサービスプロバイダーへご返品いただければ、場合により購入代金を全額払い戻しいたします。

ここで「ソフトウェア」とは関連した媒体、印刷物、「オンライン」または電子文書、すべてのアップデート、改訂、不具合修正またはモトローラまたはサービスプロバイダーから取得されたドライバを含むものとします。当社以外より提供されたソフトウェアは、そのソフトウェア製造業者から別途提供されるエンドユーザー使用許諾契約の対象となります。

このソフトウェアの所有権は当社に留保されております。モトローラは最初のお客様あるいは次のユーザーへ、本契約書の条件に従う場合に限り、個人使用に限りソフトウェアの使用を許諾します。モトローラ社とその使用許諾者がソフトウェアの所有権を留保します。

使用の許諾：

本製品の操作関連にのみ本ソフトウェアを使用してください。

本契約書の全条項に合意する場合に限り、ソフトウェア（すべてのコンポーネント・パーツや印刷物を含む）を他人へ永久的に譲渡できます。ソフトウェアを譲渡する場合、製品と（もしあれば）すべてのソフトウェア複製物を同時に譲渡するか、全複製物を破棄しなければなりません。

いかなる媒体による本ソフトウェアの原版および（もしあれば）全複製物を破棄した場合、本契約を終了することができます。

使用の制限：

(1) 上記の「譲渡」の段落にて許諾する場合を除き、他者へこのソフトウェアのすべてあるいは一部の、ローン、配布、賃貸借、リース、サブライセンスまたは譲渡はできません。(2) 個人使用目的を除き、ソフトウェアに含まれる「ユーザーガイド」を複製または翻訳できません。(3) 非互換ハードウェアで作動するソフトウェアの修正を含む（但し、必ずしもこれと限定されない）、複製、改造、翻訳、逆コンパイル、逆アセンブル、ソフトウェアのリーバースエンジニアを行うことできません。(4) ソフトウエア・プログラムおよび文書にある著作権説明やスタートアップ・メッセージを除去、改造、または非表示にすることはできません。(5) 米国のいかなる輸出法に違反するソフトウェアや製品コンポーネントを輸出することを禁止します。

本製品は、航空機のオンライン制御、航空交通、航空機ナビゲーションまたは航空機通信、ならびに原子力施設の設計、建設、運営や維持を意図とするものではありません。モトローラと第三者使用許諾者は、このような使用について明示または黙示の適切保証は致しません。本ソフトウェアをこれらの目的に使用しないでください。

すべての著作権の所有権、回路配置権、特許、商標を含む本ソフトウェアの名称、ならびに前述以外の全知的財産権、および前述の改正と修正は、いかなる場合もモトローラと第三者使用許諾者に既存します。モトローラは、本契約書に明記されていないその他のすべての権利も所有します。画像、グラフィック、写真、アニメーション、ビデオ、オーディオ、音楽を含むソフトウェアおよびその中に組み込まれる原文は、モトローラあるいは第三者使用許諾者が所有し、アメリカ合衆国所有権法と国際条約規定で保護されています。本契約書に表示記載される場合を除く、複写、模造、配分、あるいはソフトウェアの派生物、製品のいかなる部分あるいは文書は、前述の法律と条約規定にて厳密に禁止されています。アメリカ合衆国所有権法において、本契約書のいかなる項目についてモトローラが権利を放棄するものではありません。

本ライセンス、およびライセンスに記載されているお客様の権利は、米国ペンシルベニア州法に基づくものです。本契約書の条項に違反した場合、ライセンス契約は自動的に解除されます。

モトローラは、本ソフトウェアに同梱されている、またはその他の手段で本ソフトウェアとともに供給される他社製のソフトウェアについて、一切の責任を負いません。

アメリカ合衆国連邦政府の権利制限

製品および文書には権利の制限が適用されます。米国政府による使用、複製、開示に際しては、52.227-7013 の「The Rights in Technical Data and Computer Software （技術データおよびコンピュータ・ソフトウェアの権利）」条項の (c)(1)(ii) 項で規定されている制限のうち該当するものが適用されます。契約者および製造業者は Motorola, Inc., Broadband Communications Sector, 101 Tournament Drive, Horsham, PA 19044 となります。

Motorola のウェブサイトを
ご覧ください：
www.motorola.com

MOTOROLA

519101-001
10/04
MGBI